The Dialogue

Inform Engage Ideate

DATA LOCALISATION IN A GLOBALISED WORLD

An Indian Perspective

"Work purifies the heart and so leads to Vidya (wisdom)...Virtuous deeds take off the veil from knowledge, and knowledge alone can make us see God."

- Swami Vivekananda

Table Of Contents

Published on 18th November 2018

This report can be cited under the title, 'Data Localisation In A Globalised World: An Indian Perspective' - The Dialogue

About The Dialogue

The Dialogue is an emerging public-policy think-tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology, strategic affairs, sustainability and development issues.

Our aim is to enable a more coherent policy discourse in India backed by evidence and layered with the passion to transform India's growth, to help inform on public-policies, analyse the impact of governance and subsequently, develop robust solutions to tackle our challenges and capitalise on our opportunities. To achieve our objectives, we deploy a multi-stakeholder approach and work Government, academia, civil-society, industry and other important stakeholders.
Kindly visit our website at www.thedialogue.co

Project Team

Mr. Kazim Rizvi
Mr. Rohan Seth
Mr. Madhav Sharma

Support Team

Mr. Kushan Chakraborty and Mr. Siddharth Balyan

Edited by Ms. Deepanwita De
Designed by Mr. Mak Alam and Ms. Gauri Bedekar

Knowledge Partner

We would like to thank Hreem Legal, our Knowledge Partner, led by
Mr. Ashish Porwal, Mr. Majid Durrani and Mr. Diwakar Chakravorty

Acknowledgements

Over the last couple of months, more than hundred stakeholders participated to support us towards this study. While almost half of them contributed directly to the questionnaire, the rest supported us, advised us on key areas, guided our thought process and mentored us to deliver this paper. We would like to thank the government officials and the bilateral and multilateral institutions we interacted with towards the study.

We would like to take this opportunity to thank our stakeholders who supported us, starting from, in no particular order of interest, Mr. Anuraag Mehta, Mr. Jayadev Parida, Mr. Tabrez Ahmed, Ms. Meenu Chandra, Mr. Suresh Singh, Dr. Avik Sarkar, Mr. Vaibhav Chowdhary, Mr. Ranjeet Rane, Prof. Bappaditya Mukhopadhyay, Prof. Vigneswara Ilavarasan, Prof. Pooja Malik, Mr. Rishab Bailey, Dr. Parul Gupta, Mr. Vijayashankar Na, Ms. Junia Sebastian, Ms. Arya Tripathi, Ms. Ashi Bhat, Ms. Jyoti Panday, Mr. Vijeth Acharya, Ms. Kriti Trehan, Mr. Pratyush Poddar, Mr. Deepak Maheshwari, Mr. Arijit Das, Ms Swati Punia, Ms. Renjini Rajagopalan and Broadband India Forum.

This study would not have been possible without the involvement of The Dialogue's Advisory and Mentor Group and our support team comprising of Mr. Samriddh Dasgupta, Ms. Tripti Poddar and Mr. Ravish Bhatia.

Research Approach

This study has adopted different research methods to collect its findings. Broadly, the research for the study can be classified into three parts, namely, Primary Analysis, Secondary Research and analysis, and Thematic Analysis. Chapters 1-11 have been assimilated by research from various sources. Said sources are a mix of literature, legal and policy analysis as well as analysis comments we received from experts in the government, academia, civil society, and the industry. Chapter 12 is made up of analysing primary inputs through a content and thematic analysis, which is further explained in the end of the study.

Executive Summary

India is ushering into a crucial juncture, more than seventy years after independence. The country is taking important strides towards emerging as a middle-income economy, provide jobs to millions of people, take global leadership on issues of geopolitical importance and stake claim for a growing superpower. In all of this, data and technology will play a fundamental role for India going forward.

If the 20th century brought the promise of the Internet as a decentralised and self-regulating space, the 21st century is marked by battles over the control of data.

This study aims to study the impact of data localisation from various perspectives, analyse the government's objectives towards implementation of such policy, identifies alternate policy mechanisms that we believe are better suited to drive home the objectives as opposed to blanket data localisation.

Cross-Border Data Flow fundamental

The cross-border data transfer is a multidimensional concept, which involves international stakeholders and cooperation in data processing storage, retrieval and transmission borders. The ability to move data globally at the given time has been very central to the global economic order and a legislation with a data localisation restricting the movement of data could become a burden for MNCs across all sectors of economy.

The data localisation may act as a trade barrier and restriction and challenge the free market economy. The restriction imposed may lead to the decrease in the foreign direct investment in India or in rarest of rare case, a trade war of the data.

Huge Costs to Mandatory Data Localisation

The cases around world also suggest that the data localisation comes with a huge cost. The European Centre for International Political Economy - ECIPE 2014 studied the estimated cost and challenges to set up the data centres in a country among those are the following: estimated GDP loss of 0.8%, reduced growth by 20%, decrease in FDI by 1.9% (Europe). Economy-wide data localisation requirements have led to a negative impact on GDP in several countries where such requirements have been considered (Brazil -0.8%, India -0.8% and Republic of Korea -1.1%) or implemented (Indonesia -0.7%). This would have the effect of making services more expensive for customers.

Organic Data Storage through progressive policies

Rather than forcing companies to store data in India, the government should look at pursuing strategies incentivize the growth of the data industry in India. India should look at promoting investments in the entire value chain, including manufacturing storage devices and establishment of local data centers.

Alternative Policy Mechanisms

While we understand and agree with the Government's objective to enable India a data independent country, mandatory localisation is probably not the best way to go about it. Instead, we have identified certain alternate policy measures that can help achieve similar objectives around data access for law enforcement purpose, reforming the MLAT, moving towards a multilateral framework for

global privacy standards and qualifying the adequacy test under the CLOUD Act and EU GDPR; data sharing agreements with leading countries and other progressive policy measure to incentivise storage in India. Similarly, to make data localisation a success, India will have to implement a due process of law for domestic data access as blanket implementation of localisation without any process will go against the spirit of privacy as enshrined by the Supreme Court in the Puttaswamy judgement last year.

For our policy-makers, the important question to ask is: Whether localisation is the least Is the least coercive policy to achieve the intended objectives? Our research carried over the span of more than two months, comprising of primary and secondary data analysis, discussion with leading government, bilateral, civil-society, academia and industry stakeholders suggest that this is not the case. On one hand India is opening its doors to the world seeking greater investments and trade, while on the other hand restrictive policy measures such as data localisation will harm the economy in the short to medium term. It is bound to impact the investor;s sentiments and we can only hope that this policy will have minimal impact on the country's growing IT sector. India will have to carefully balance the enforcement benefits of data localisation with the costs involved pursuant to such requirement.

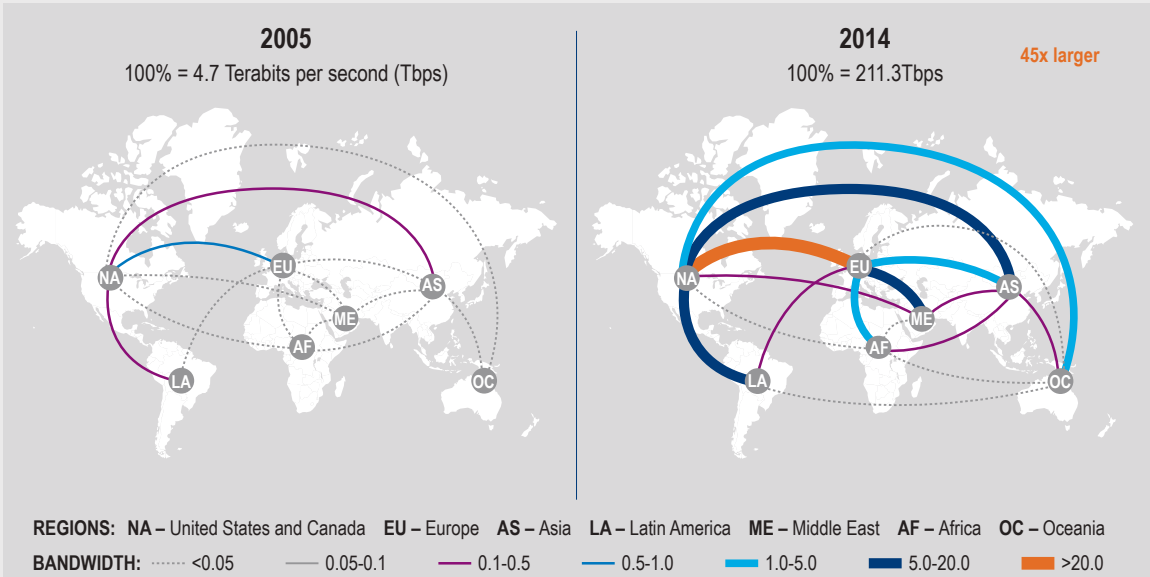
CHAPTER 1

CROSS-BORDER DATA FLOWS AND WHY THEY MATTER

1.1 Globalisation of Data: A Reality

In the modern age of global trade, cross-border data flows play an instrumental role in the management and security of the movement of goods and services. Data and the digital economy are inextricable aspects of a nation's economic growth and development. The space-time compression offered by emails and phone calls speeds up and facilitates decision-making. This ensures well-informed growth at unprecedented speeds. At the crux of this digital economic growth, lie global data flows. Data continues the impact it has been able to make as a virtue of the pace at which it is shared.[1]

These flows have boosted production across-borders. The GSM Association (a consortium of more than 750 operators and over 350 telecom companies[4]) claimed that data flows account for $2.8 trillion of the global GDP in 2014[5]. While the numbers themselves are telling, they do not do justice when describing the impact of data. Transborder data flows acutely impact the ability of firms to conduct business internationally. Freer and faster flow of data contribute significantly to the functioning of businesses and whole sectors. Business Roundtable, self-defined as an association of CEOs of leading American



Source: Digital Globalization: The New Era of Global Flows, McKinsey Global Institute, 2016

Image 1. Growth of Cross Border Data Flows 2005-14 [2]

Companies and governments around the world have used this to advance their progress. How else can one explain the rise of data flows in the past decade and a half? McKinsey Global Institute claims that growth in data flows increased 45 times between 2004 and 2014[3] as shown in Image 1.

companies[6], identified six mechanisms through which cross-border data flows help businesses in other sectors, namely, interconnected machinery, back-office consolidation, supply-chain automation, digital collaboration, cloud scalability, and big data analytics[7]. Hence, the impact of cross-border data flows could be well beyond $2.8 trillion.

Not only is the impact sizeable, but its distribution is also unique when compared to the distribution of 'traditional' goods. Countries at the center of the traditional flow of goods had the most to gain from trade. They benefit from the convenience of their location and can have cheaper access to commodities such as imported fruits. However, data flows do not necessarily adhere to the same logic. The costing for data transfer is much more efficient. Even countries at the periphery can send and receive data at minimal costs, regardless of their location. Because of that, they might stand to gain even more than those at the center[8]. Because of enhanced accessibility, the arrival of new digital platforms has the potential to be transformational for countries that were deprived of them before.

[1] "*Regulating for a digital economy: Understanding the importance of ....*" *20 Mar. 2018, https://www.brookings.edu/research/regulating-for-a-digital-economy-understanding-the-importance-of-cross-border-data-flows-in-asia/. Accessed 15 Nov. 2018.*
[2] "*Global Working Papers - Brookings Institution.*" *https://www.brookings.edu/series/global-working-papers/. Accessed 15 Nov. 2018.*
[3] "*Digital globalization: The new era of global ....*"
https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows. Accessed 26 Oct. 2018.
[4] "*About Us - GSMA.*" *https://www.gsma.com/aboutus/. Accessed 26 Oct. 2018.*
[5] "*Regional Privacy Frameworks and Cross-Border Data Flows - GSMA.*"
https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf. Accessed 26 Oct. 2018.
[6] "*Business Roundtable.*" *https://www.businessroundtable.org/. Accessed 26 Oct. 2018.*
[7] "*The Global Information Technology Report 2016.*" *https://www.wsj.com/public/resources/documents/GITR2016.pdf. Accessed 26 Oct. 2018.*
[8] "*digital globalization: the new era of global flows - McKinsey & Company.*"
https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx. Accessed 26 Oct. 2018.

1.2 Cross-Border Data Flow Fueling Global Economies

A popular saying today is that data is the new oil[9]. The idea is that data, in the future, will have a role to play on par with the role oil had played in driving the third industrial revolution. While there is little doubt on the importance of data in driving the global economy forward, one would be mistaken to assume that data's role is yet to come. There are several indications in favour of the idea that data and digitization have begun to drive the global economy now, not years down the line.

Let's consider American exports in 2012. A report by the World Economic Forum stated that 61% (US$383.7 billion) of American service exports were delivered digitally in 2012. Imports followed suit. The US received 53% of its imports digitally[10]. The EU has even higher amounts of digital imports and exports (in absolute terms). The supra-state delivered $465 billion worth of exports digitally. As argued before, these numbers do not do justice to the broader impact cross-border digital imports and exports have on the global economy. These flows do not just impact the technology sectors in their respective countries but go on to affect other sectors as well. Other, non-technology sectors capture an approximate 75% of the internet's benefit[11].

The impact of the cross-border data flows is so fundamental that changing or attempting to restrain facets of it can adversely affect a country's GDP as well as FDI. A report by the European Centre for International Political Economy (ECIPE) claimed that should Indonesia pursue data localization laws their GDP would reduce by 0.7% and investments by 2.3%[12]. Similarly, trying to restrict the potential of data would have adverse effects across the board should they be followed by relatively more developed economies such as the EU or South Korea.

Cross-border data flows have fuelled progress on an unprecedented scale. A key feature of this phenomenon is the defiance of physical borders in how they operate. There is a case to be made that the current benefits of cross-border data flow that fuel today's progress is just the beginning. The prospects of what these data flows can accomplish in the future are boundless[13].

[9] "*Data Is the New Oil of the Digital Economy | WIRED.*"
https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/. Accessed 26 Oct. 2018.
[10] "*Cross-Border Data Flows, Digital Innovation, and Economic Growth ....*"
http://www3.weforum.org/docs/GITR2016/WEF_GITR_Chapter1.2_2016.pdf. Accessed 26 Oct. 2018.
[11] "*Internet matters - McKinsey & Company.*"
https://www.mckinsey.com/~/media/McKinsey/Industries/High%20Tech/Our%20Insights/Internet%20matters/MGI_internet_matters_exec_summary.ashx. Accessed 26 Oct. 2018.
[12] "*The costs of data localisation: friendly fire on ... - ECIPE.*"
http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf. Accessed 26 Oct. 2018.
[13] "*Cross-Border Data Flows: Realising benefits and removing barriers ....*" *5 Sep. 2018,*
https://www.gsma.com/publicpolicy/cross-border-data-flows-realising-benefits-and-removing-barriers. Accessed 15 Nov. 2018.

1.3 Big Data Analytics – The Future of Global Trade

Wondering how data might lead us in the coming years automatically brings up the mention of big data analytics. It is the practice of analyzing large data sets to develop insights. These insights can be fundamental to how a business operates and expands. For instance, consider if an airline wished to open a new route from Kanpur to Varanasi. It would check the number of passengers commuting through the route through the train and the price they were willing to pay. It would need huge datasets from Indian Railways and bus

Image2. The amount of data produced every day across the world

services to justify whether or not servicing the route would be a good idea. The datasets in this scenario are 'Big Data,' and the practice of deriving insights from it is called 'big data analytics.'[14]

Insights such as the one above prove that big data has the potential to drive innovation, growth, and economic competitiveness. It would lead to smart allocation of resources and also, more relevant advertisements. This is a segment that is projected to grow substantially shortly. That is not to say that it is not sizeable already. Forbes recently reported that 2.5 bytes were being produced every day[15].

Insights from big data analytics not only help businesses expand, but they also guide decisions in daily life. Data generated and transferred across borders has proven to be indispensable to simplify daily life today. For example, just collecting and analysing locations through phones allows Google Maps helps determine the best (if not the shortest) path from point A to point B. Insights developed help users remotely check for traffic congestion as well as quantifies the amount of time it might take after considering the dynamic situation on the ground in real time[16].

Similarly, insights generated through big data analytics are helpful to streamline research and development, decision making and customer satisfaction. Big data enables companies to identify patterns of demand and larger business environments. Not only do these insights make for faster advancements in products, but also allows companies to respond to changes as (or before) they occur. BMW recently leveraged this to their advantage by creating an "idea management system" to evaluate ideas submitted through its "virtual innovation agency." Collecting this data reduced the company's time spent on identifying high-potential ideas by 50%, and led it to annually incorporate two to three ideas from the open innovation effort into new car models[17].

While insights from big data are already driving innovation and growth, it is important to remember that big data is still expanding. According to one estimate in 2013, 90% of all the data in the world had been created only in the previous two years[18]. Over time, as big data grows, more trends and insights are sure to emerge. Moreover, as they do, global trade will benefit, and more will ride on the free flow of data than ever before.

Image 3. About 80 percent of the data generated by businesses is unstructured which is why big data analytics and AI have emerged as strategic assets[19]

[14] "*Big data analytics: What it is and why it matters | SAS.*" *https://www.sas.com/en_us/insights/analytics/big-data-analytics.html. Accessed 15 Nov. 2018.*
[15] "*How Much Data Do We Create Every Day? The Mind-Blowing Stats ....*" *21 May. 2018, https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/. Accessed 26 Oct. 2018.*
[16] "*Traffic Congestion and Reliability: Linking Solutions to Problems.*" *https://ops.fhwa.dot.gov/congestion_report_04/executive_summary.htm. Accessed 15 Nov. 2018.*
[17] "*New Themes in Innovation Policy – New ... - INNOGRIPS Logo.*" *http://innogrips.empirica.biz/fileadmin/innogrips/documents/01_policy%20briefs/ig_policybrief_6_new-themes.pdf. Accessed 26 Oct. 2018.*
[18] "*Big Data, for better or worse: 90% of world's data ... - ScienceDaily.*" *22 May. 2013, https://www.sciencedaily.com/releases/2013/05/130522085217.htm. Accessed 26 Oct. 2018.*
[19] "*Bengaluru: what's next for India's tech capital? | Business to business ....*" *3 Jul. 2018, https://www.theguardian.com/business-to-business/2018/jul/03/bengaluru-whats-next-for-indias-tech-capital. Accessed 1 Nov. 2018.*

1.4 India's Digital Renaissance Founded on Cross-Border Data Flow

Current developments in the potential of data and the promise of more to come in the future make it imperative for developing economies like India to leverage this opportunity towards fuelling their progress.

India is no stranger to leveraging opportunities to achieve progress. The emergence of Bangalore as a technology hub is a testament to that[20]. India today is a global hub for business process outsourcing. According to a survey by Deloitte, 59% of the businesses interviewed were outsourcing their operations to India. More than a fifth of those interviewed (22%) were considering making a move[21]. Apart from outsourcing of business operations, there has been significant growth in India's IT sector, with the $167 billion IT services industry projected to expand at a rate of 7-9 % in 2019[22]. MNC branches in India offer their services globally and benefit from the free flow of data that enables them to do so.

A similar shift might be imminent regarding leveraging data flows to the benefit of the Indian IT industry. Indian companies have been benefitting from the free flow of data. Myntra and RedBus, for instance, have hosted their data servers with global providers such as Amazon Web Services[23]. Fortis Healthcare, in a bid to save costs, relocated their data center abroad (Windows Azure Cloud Service)[24] while Flipkart (recently acquired by Walmart) too, during its early days, relied on Canadian servers for operations.

Outsourcing data storage needs can help save on costs while building data centers can help drive investment. Both these options should appeal to India as she strives to move towards a 'digital economy.' With the push for cashless payments and smart cities, cross-border data flows would be instrumental in achieving all of these goals.

To that extent, rapid growth is expected from internet related businesses with projections claiming 3.2% contribution to the Indian GDP[25]. As the fourth industrial revolution gets underway, India is faced with the option to leverage advancements in technology to facilitate its growth. If utilized well, cross-border data flows could help fuel the digital renaissance of the Indian economy.

[20] *"Bengaluru: what's next for India's tech capital? | Business to business ...." 3 Jul. 2018, https://www.theguardian.com/business-to-business/2018/jul/03/bengaluru-whats-next-for-indias-tech-capital. Accessed 1 Nov. 2018.*

[21] *"Outsourcing to India | Whitepaper - Back Office Pro." https://www.backofficepro.com/white-paper/outsourcing-to-india/. Accessed 26 Oct. 2018.*

[22] *"Nasscom: Indian IT to clock 7-9% growth in FY19, job creation to ...." 20 Feb. 2018, https://economictimes.indiatimes.com/tech/ites/indian-software-services-sector-to-grow-7-9-in-fy19-nasscom/articleshow/62995685.cms. Accessed 26 Oct. 2018.*

[23] *"July 25, 2016, Shri A. Robert J. Ravi Advisor - Telecom Regulatory ...." 25 Jul. 2016, https://trai.gov.in/sites/default/files/201609070951396640421ITI_0.pdf. Accessed 26 Oct. 2018.*

[24] *"Public Cloud Powers Business Transformation at Healthcare Major ...." https://enterprise.microsoft.com/en-in/customer-story/industries/health/public-cloud-powers-business-transformation-healthcare-major/. Accessed 26 Oct. 2018.*

[25] *"The Rise in Internet Penetration and the Changing Face of Digital India." 27 Jan. 2015, http://www.iamwire.com/2015/01/rise-internet-penetration-changing-face-digital-india/108808. Accessed 26 Oct. 2018.*

1.5 Cross-Border Data Flows Key to Developing 4th Industrial Revolution

Reflecting upon previous industrial revolutions, a pattern seems to emerge. The first revolution was powered by steam to enhance production capacity. The second was facilitated through electric power as it created avenues for mass production. The third moved toward automation with electronics and IT. Industry 4.0 promises to build on the computerization of the third revolution through the internet of things and big data analytics. At the core of the latter, data will serve as the guiding force.

The importance of the ability to share data perhaps only second to the importance of the existence of the data itself. A key reason why data is so valuable is that it can be shared at unprecedented speeds, paying little heed to national borders. As a result of high-speed cross-border data flows, companies have been able to optimize their services. Cloud computing services are the best exhibit for the same. Companies can provide cheap, on-demand computing capability to big and small businesses alike. Thanks to this, small and medium firms can avail world-class cloud computing services according to the computing power they need. Whole sectors such as supply chain management are being transformed. Scaling in industry 4.0 is cheaper than ever before. For a quantification, look no further than DHL's estimation that IoT technologies will have an impact of more than $1.9 trillion on supply chain management and logistics[26].

While DHL's scale is macro, the micro effects of industry 4.0 are likely to be equally transformative. Unlike the revolutions that came before it, the impacts of changes in industry 4.0 are felt at unprecedented speed to the individual as well as the business. However, it is crucial to remember that scaling and automating at such affordable costs is a product of reducing costs at the back end. Moreover, cross-border data flows are essential to keeping these costs down while simultaneously contributing to innovation and efficiency.

[26] "*Internet of Things Will Deliver $ 1.9 Trillion Boost to Supply Chain and ....*" *16 Apr. 2015, https://www.businesswire.com/news/home/20150416006351/en/Internet-Things-Deliver-1.9-Trillion-Boost-Supply. Accessed 26 Oct. 2018.*

1.6 Transforming the Nature of Digital Trade

Cross-border data flows are causal in disrupting global trade thanks to the rate of internet penetration globally. In the developing world internet penetration averages around 41 percent compared with 81 percent in the developed world[27]. With numbers such as these, it is no surprise then, that the popularity of digital imports and exports has mushroomed internationally.

Digitization of trade is the apparent effect cross-border data flows have on economies, but it is not the only one. Another critical factor worth mentioning is the cross-border platform data flows provide to small and medium-sized firms, enabling them to engage in international trade. Companies today have the potential to establish a presence internationally without having a physical base. This is particularly helpful for start-ups which relocate limited funds to other uses. In addition to the ability to gather a global presence, cross-border data flows provide small businesses with online services such as cloud computing and knowledge repositories that are vital for business development and communications.

Apart from being an enabler for small businesses, cross-border data flows to serve as the ideal platform to facilitate online advertisements, which re-shapes global trade and connectivity. At the back end, transfer of the data collected through mobile devices and sensors is monetized through firms such as Google and Facebook. This allows them to serve their consumers without an upfront fee and tailors the advertisements keeping in mind the preferences of each consumer. Advertisements allow global firms to reach consumers through their smartphones, regardless of their location. This makes for better consumer awareness and more intense market competition. In turn, advertisements have a sizeable contribution in facilitating connectivity[28].

[27] *"Press Release: ITU releases 2016 ICT figures ...." 22 Jul. 2016, https://www.itu.int/en/mediacenter/Pages/2016-PR30.aspx. Accessed 26 Oct. 2018.*
[28] *"A brand new game - Marketing in the digital age - The Economist." 27 Aug. 2015, https://www.economist.com/business/2015/08/27/a-brand-new-game. Accessed 15 Nov. 2018.*

1.7 Measuring the Impact of Cross-Border Data Flows

Measuring how important cross-border data might be to the global economy is a complicated task. Not least because data flows and digital trade might be inseparable from the 'traditional' economy. It would be hard to imagine how industries such as consulting and banking might function without international communication.

The World Bank came up with a study using data from 2001 to 2013 to measure the impact of internet penetration on bilateral trade. The study concluded with the insight that a 10% rise in internet penetration in the exporting country drives a 1.9% increase in the number of goods being exported. Similarly, a 10% rise in internet penetration in the importer led to a 0.6% increase in the average value of goods[29].

Quantifying the impact of cross-border data flows on different economies would not do justice to the ripple effect these flows have on whole sectors. For instance, this chapter has explored themes on how cross-border data flows play a role in digital imports and exports, supply chain management, logistics, enabling small businesses, big data analytics for the individual and the industry, cheaper scalability, cloud computing, and online advertisements. However, there may well be more avenues for cross-border data flows alive today before we begin to count the uses that might emerge in the future.

One thing that is clear, however, is that cross-border data flows are worth keeping. India has a stake in what these flows can produce next, and by extension, so does industry 4.0.

[29] "*World Bank Document - Open Knowledge Repository.*" *https://openknowledge.worldbank.org/bitstream/handle/10986/24866/WPS7785.pdf. Accessed 26 Oct. 2018.*

CHAPTER 2

DATA LOCALISATION DRIVING DOMESTIC PROTECTIONISM

2.1 Introduction

Data localisation is defined as the act of storing data on any device that is physically present within the borders of a specific country it was generated. Free flow of digital data, especially data which could impact government operations or operations in a region, is restricted by some governments[30].

For all the pros that come along with cross-border data flows, their effectiveness is being challenged by global data localization laws. Countries around the world have installed localization laws in some form or the other. Russia's Federal Law No. 242-FZ came into effect in September 2015[31]. The legislation compelled companies to gather, store, and process the personal data of its residents using the data servers located in the country[32]. China too came out with a comprehensive but ambiguous data localization law in 2017. In a bid to achieve "cyber sovereignty," the law forbade banks and other financial institutions to store abroad any personal financial data that they collected in China. It also requires service providers to store any 'important data' collected within China unless they passed a security assessment. Interestingly, the phrase 'important data' replaced 'critical information infrastructure' in the law, presumably allowing the government to broaden its scope of authority and strengthening leeway for unrestricted government intervention in any industry[33].

Australia too has dabbled in data localization to some extent by implementing the Personally Controlled Electronic Health Records Act in 2012. According to the law, operators with access to individual or public health records cannot transfer them outside the country[34]. There are other instances of countries using data localization to serve their domestic interests. Vietnam, Nigeria, and Indonesia are all examples of the same[35].

Efforts at localizing data flows as a means of policy have varied in their approach and gravity. Australia's approach was focused only on healthcare while China's law falls at the other end of the spectrum.

[30] *"What is Data Localization? - Definition from Techopedia." https://www.techopedia.com/definition/32506/data-localization. Accessed 15 Nov. 2018.*
[31] *"Russia Data Localization Requirement at a Glance - Bryan Cave Data ...." http://bryancavedatamatters.com/wp-content/uploads/2015/05/Russia-Data-Localization-Requirement-at-a-Glance.pdf. Accessed 26 Oct. 2018.*
[32] *"Federal Law No. 242-FZ. | wilmap." 14 May. 2018, https://wilmap.law.stanford.edu/entries/federal-law-no-242-fz. Accessed 26 Oct. 2018.*
[33] *"Chinese Data Localization Law: Comprehensive but Ambiguous - The ...." 7 Feb. 2018, https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/. Accessed 26 Oct. 2018.*
[34] *"A Data Localization Free-for-All? | Center for Strategic and ...." 9 Mar. 2018, https://www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/data-localization-free-all. Accessed 26 Oct. 2018.*
[35] *"Data localisation norms could negatively impact India's GDP | analysis ...." 20 Jul. 2018, https://www.hindustantimes.com/analysis/data-localisation-norms-could-negatively-impact-india-s-gdp/story-A8HNFTjIDBM550HJiKbpnO.html. Accessed 1 Nov. 2018.*

2.2 Multiple Levels of Localisation

As an end goal, there are many ways to 'secure' data, some more stringent than the others. Moreover, countries choose to apply these methods as a blanket regulation or can even go for more sector-specific approaches. Listed below are the four main categories of data localization in order of most stringent to least stringent[36] :

2.2.1 Geographical restrictions on data export

This form of restriction mandates that the data itself or any of its copies not be allowed to leave the territory. If enforced, it compels foreign companies to create or rely on servers located within the country and develop infrastructure to maintain the data. As described at the beginning of this chapter, China imposes a version of this variant to maintain its data sovereignty[37].

2.2.2 Geographical restrictions on data location

This form of data localization requires companies to retain a local replica of the data. So while copies of the data can leave national borders, an updated version of the data should always reside within the country. Indonesia and Malaysia impose such rules on businesses operating within their borders.

2.2.3 Permission-based regulations

This variant of data localization mandates that foreign entities must seek consent from their consumers before approving a cross-border data transfer. Brazil and Switzerland follow a variant of this.

2.2.4 Standards-based regulations

This is arguably the least severe form of regulation. Foreign entities are allowed to transfer data across-borders freely. The only condition they must fulfill is to meet the security standards set by the country/region the data is collected from to ensure security and privacy for customers.

Each of these approaches is not blanket regulations per se and can vary depending on the 'sensitivity' of data. For instance, consider the approach taken by the white paper presented by the Srikrishna committee. While data regarding citizen's health falls under the most stringent form of regulation (extenuating circumstances aside), other personal data of citizens may be subject to cross-border flow by meeting obligations set under model contract clauses.

[36] "*Addressing the Impact of Data Location Regulation in Financial Services.*" *22 May. 2015, https://www.cigionline.org/publications/addressing-impact-data-location-regulation-financial-services. Accessed 26 Oct. 2018.*

[37] "*Chinese Data Localization Law: Comprehensive but Ambiguous - The ....*" *7 Feb. 2018, https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/. Accessed 30 Oct. 2018.*

2.3 Rising Trend of Data Localization

In this section, we analyse the reasons and justifications governments provide in order to adopt localisation measures.

2.3.1 Geopolitical Concerns

Ever since the National Security Agency (NSA) had many of its secret surveillance programs revealed to the public in 2013[38], several governments have responded by way of stricter regulation. Most of the new laws are aimed at protecting countries from foreign interception and surveillance by preventing sensitive data from leaving the domestic territory.

Governments view data localization as a means to ensure safety and protection of data in the event of a global geopolitical crisis. For instance, a significant amount of cross-border data flow is managed through undersea cables. This is viewed as a concern because the location of almost every undersea cable in the world is publicly available.

While there is a broad acknowledgment that the likelihood of such a situation is low, this concern remains persistent. Moreover, data localization is seen as a step to avoid the vulnerabilities of relying on the fiber optic cable network[39].

2.3.2 Foreign Surveillance

A significant reason why the Indian government is pushing for data localization is to prevent foreign surveillance. This rationale is evident in the Shrikrishna committee's recommendations to keep data relating to the state's critical interests within its borders[40]. While such critical data is to be exclusively processed in India, all other kinds of data might remain freely transferable, under the assumption that certain conditions for cross-border data flow are met.

There is a debate on how useful this measure would be in stopping data from threats. While the presence of physical servers inside national borders might be useful in stopping foreign surveillance, it might also make the servers more vulnerable to domestic threats. Also, because of India's available, scalable infrastructure (or lack thereof), the presence of data centers in the country might compromise on the quality of the same.

2.3.3 Protectionism

The Srikrishna committee white paper does not exclusively mention the term protectionism, and neither does it discuss its impact on the domestic data industry vis-à-vis protectionism in great detail. However, that should not downplay the potential data localization has to damage the capacity and quality of the Indian data storage and processing industry.

Localisation, in its most severe form, could make the domestic data storage providers less competitive. By taking out world-class international alternatives, the industry would be deprived of incentive to grow and offer better services at lower prices. Not only will that be counterproductive to the needs of the growing Indian businesses but will also discourage foreign investors from considering India as an option[41].

Moreover, while the white paper does not call for such severe localization, it can serve as a gateway to protectionism through future amendments. This has the potential to shape India's role in industry 4.0 going forward.

2.3.4 Access to data crucial for governments:

Governments have reason to believe that access to data is more comfortable when the data resides locally, for civil and criminal investigations on a variety of issues. Recently, issues such as black money, corruption, and high-profile banking scams have led to the government exercising greater scrutiny, particularly on financial transactions by Indian citizens. As a result, RBI has been leveraging companies to provide "unfettered supervisory access" to their data on payments, customers, and all transactions[42].

Another lens to justify the unfettered access to data is that of effective law enforcement. The rationale behind placing data servers inside a country's territory is that it becomes easier for law enforcement agencies to gather evidence. Should the information be within their jurisdiction, it makes for easier and faster access as compared to the tedious processes agencies might have to go through in cases where the data is stored internationally.

The Srikrishna committee does acknowledge that keeping the data servers in India might not be the perfect workaround for the same[43]. Particularly so when the data might be under the jurisdiction of foreign entities even as it stays in India. However, domestically locating the servers does come with the added advantage that the possibility of a foreign bodies declining access to their data would be diminished.

2.3.5. Economic Development and Exploring Analytics:

Another argument behind data localization mandates is "data mercantilism"[44], an open government policy to promote economic advantage by favoring local industries. There is a full belief that localizing data within national borders will increase investment locally. Thus, data localization measures are often motivated, whether explicitly or not, by desires to promote domestic economic development.

[38] "*Edward Snowden: Leaks that exposed US spy programme - BBC News.*" *17 Jan. 2014, https://www.bbc.com/news/world-us-canada-23123964. Accessed 30 Oct. 2018.*
[39] "*The Debate – Data Localization And Its Efficacy - Data Protection - India.*" *17 Sep. 2018, http://www.mondaq.com/india/x/736934/Data+Protection+Privacy/The+Debate+Data+Localization+And+Its+Efficacy. Accessed 26 Oct. 2018.*
[40] "*White Paper on Data Protection framework for India - Public ... - MeitY.*" *18 Dec. 2017, http://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited. Accessed 1 Nov. 2018.*
[41] "*The Global Risks Report 2017 12th Edition - World Economic Forum.*" *4 Nov. 2016, http://www3.weforum.org/docs/GRR17_Report_web.pdf. Accessed 15 Nov. 2018.*
[42] "*Reserve Bank of India - Notifications.*" *6 Apr. 2018, https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0. Accessed 30 Oct. 2018.*
[43] "*The Debate – Data Localization And Its Efficacy - Data Protection - India.*" *17 Sep. 2018, http://www.mondaq.com/india/x/736934/Data+Protection+Privacy/The+Debate+Data+Localization+And+Its+Efficacy. Accessed 1 Nov. 2018.*
[44] "*Localization Barriers to Trade: Threat to the Global Innovation ... - ITIF.*" *1 Sep. 2013, http://www2.itif.org/2013-localization-barriers-to-trade.pdf. Accessed 1 Nov. 2018.*

2.4 Factors Determining Storage of Data

Because the transfer of data is not governed under the same conditions as those of most other goods, it is worth looking at different factors that go into deciding where the data servers are located. The following is a brief of conditions that might play a part in determining the optimum location of data servers. A comprehensive breakdown of some of the factors is available in Chapter 9.

2.4.1 Environmental efficiency:

Cooling is a significant cost in data center operations. Because of this some climates are better suited than others for the efficient functioning of data centers[45].

2.4.2 Limits of Communication Technology:

Availability of networks and bandwidth is critical when deciding where to set up a data storage and processing facility. Some locations are better connected and can, therefore, provide higher quality services.

2.4.3 Physical and Political Security:

While it is essential to maintain cheap and efficient data storage solutions, it might be rendered futile if the physical safety of the location is not ensured. In order to provide end users with the best solutions, it is paramount to keep data centers away from regions prone to conflict and political instability.

2.4.4 The Demographics:

While setting up data centers, it is essential to take into account where the end users are located. In addition to the same, it is also worth knowing their computing requirements.

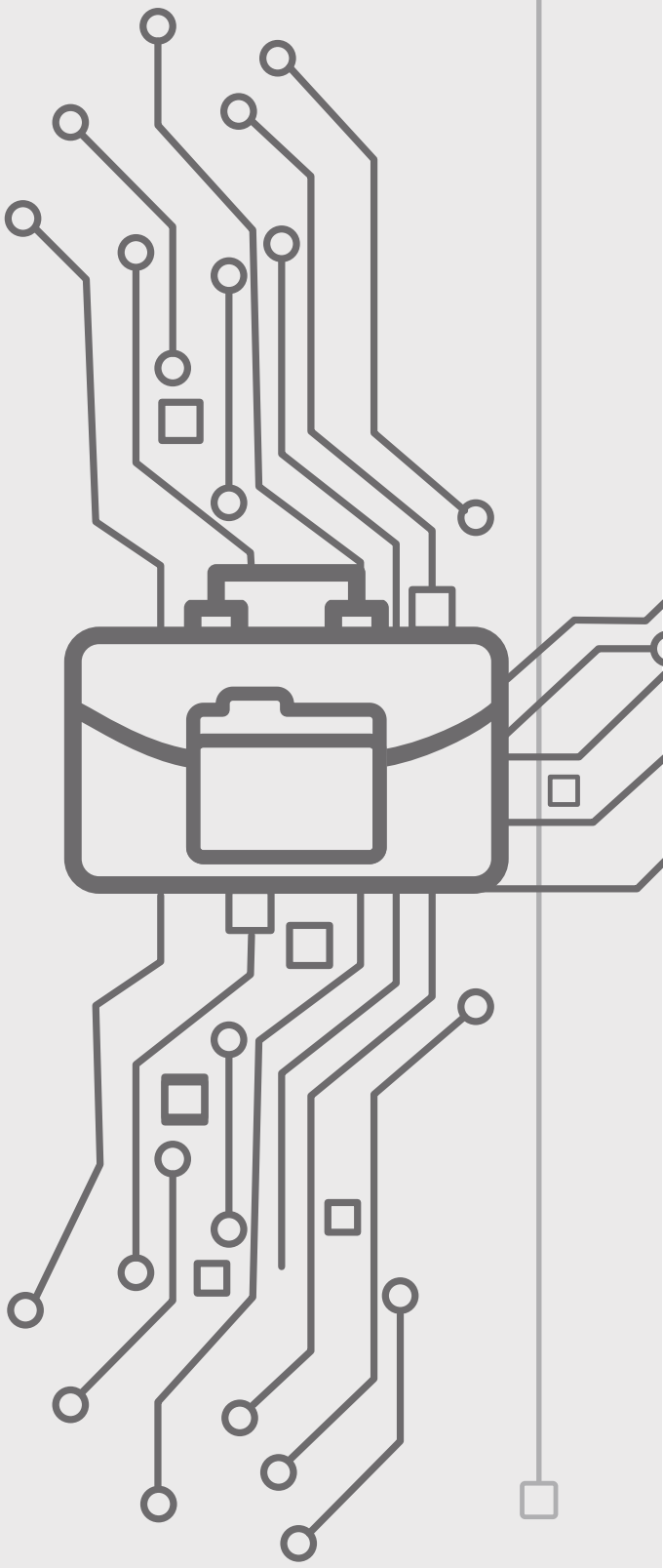
2.4.5 Financial Considerations:

Perhaps the most obvious variable is financial viability. The availability of cheap space, power, and communications serve as an excellent base to set up a data storage and processing center. While this is a sizeable list of factors that go into determining the physical location of data storage, it is by no means exhaustive. There may well be more factors depending on the favorite combination of conditions and resources available to a company.

[45] "*Best Practices for Data Centers: Lessons Learned from ... - CiteSeerX.*" *http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=AB9AA88224E428BCB86D9EEB836F41D8?doi=10.1.1.207.3280&rep=rep1&type=pdf. Accessed 15 Nov. 2018.*

CHAPTER 3

SUB-OPTIMAL IMPACT OF FORCED DATA LOCALISATION



3.1 Introduction

In the first chapter, we discussed the benefits of cross-border data flows and how they fuel the global economy. In the second chapter, we identified the concept of localization and the trends around the same. This chapter will focus on the impact data localization policies can have when forced on the industry. Localisation is not a monolith, and its effects differ based on where localization is implemented. The authors are of the opinion that organic storage based on market forces is an effective way to go about the process.

Matthias Bauer, Martina Ferracane and, Erik van der Marel claim in their study that data regulations in general and data localization requirements, in particular, can take different forms according to stated objectives and this can affect downstream industries in many different economically distorting ways[46]. Data localization has the potential to threaten progress by hindering the development of goods and services and slowing economic growth.

It is essential now more than ever to bring this to light as the number of data localization measures are on the rise globally. As countries begin to realize the importance of data, they come out with policies to contain its potential. A telling statistic in this regard comes from The European Centre for International Political Economy (ECIPE). The think tank calculates that in the decade to 2016, the number of significant data localization measures in the world's large economies increased almost threefold, from 31 to 84[47].

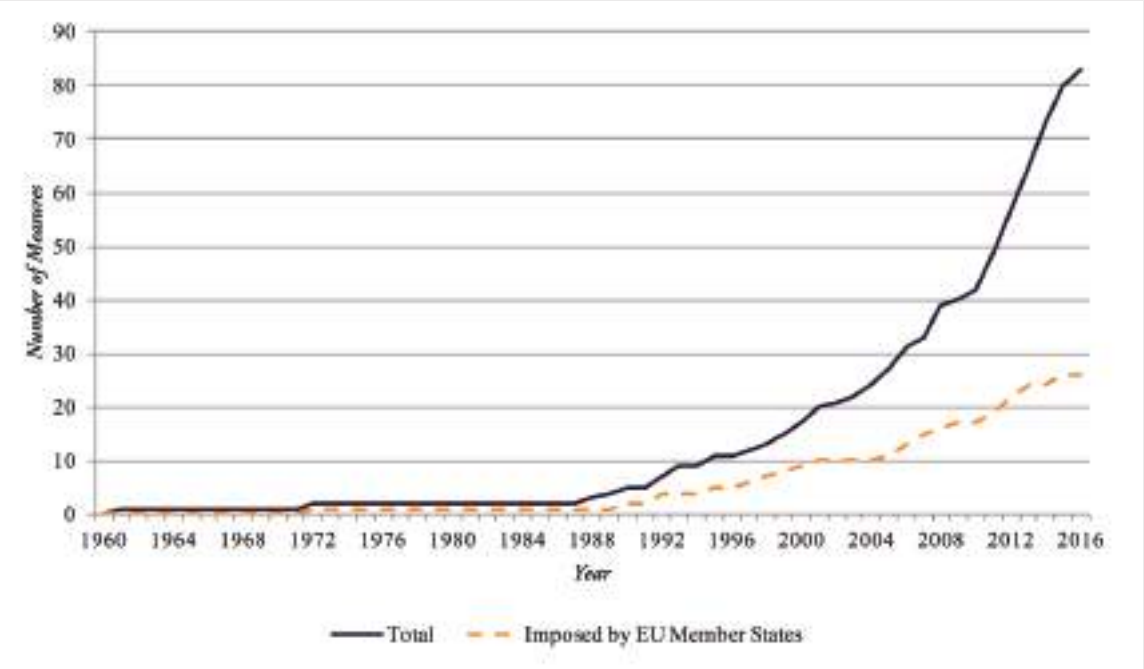


Chart 1: Number of data localisation measures implemented globally and intra-European Union from 1960-2016

The oldest measure – which actually pre-dates the internet, but is enforced online was implemented as early as 1961. Until 2000, only 15 measures were imposed globally. By 2008, the number of measures doubled and it more than doubled again until today[48].

Increase in data localization laws will affect different sectors of the economy. According to a study conducted by the British think tank Chatham House and the Centre for International Governance (CIGI), data localization laws have had adverse effects on the Indian economy. The study claims that the regulations have increased prices and decreased productivity in India, resulting in a loss of 0.25% of real GDP annually. The study also quantified total factor productivity (TFP) costs that India will incur due to the new regulations. The losses are expected to be around 1.35% in the communications sector, 0.50% in the ICT business services sector, and 0.20% in the finance and insurance sector[49].

There is a lack of evidence that data localization requirements serve to improve data protection. On the contrary, there is a case to support the argument that localization can disrupt operations of both fiduciaries & processors and will have a negative impact on any economy it is implemented in. For instance:

• In many cases, it is not possible to process all data locally and maintain the same quality of service as could otherwise be achieved (for example, round-the-clock, follow-the-sun customer service). This is essential for companies that operate globally and follow different markets, like Deutsche Bank.

• The trend towards micro-services in service architecture and increasing distribution of data processing means that data localization restrictions are likely to result in companies choosing not to serve the Indian market or significantly reducing the functionality of their services.

• Data localization restrictions risk significantly impairing innovation by raising costs to potentially prohibitive levels for small and medium enterprises[50].

• Data localization restrictions will undermine India's ability to leverage emerging technologies that rely significantly on global networks, like cloud computing and AI[51].

It could affect access to transborder media and applications – particularly insofar as smaller content providers are concerned.
This chapter will focus on identifying the impact data localization can have when forced on the industry. This will include examining the economic cost of localization, the organizational complexities that stem from it, impact on efficiency, reduction of the global footprint, reduced access to financial services & challenges to global technology strategies.

[46] *"Unleashing Internal Data Flows in the EU: An Economic Assessment ...." https://bit.ly/2gYUfDQ. Accessed 26 Oct. 2018.*
[47] *"TODAYonline | Data protectionism: the growing menace to global ...." 20 May. 2018, https://bit.ly/2zXuNFJ. Accessed 26 Oct. 2018.*
[48] *"Unleashing Internal Data Flows in the EU: An Economic ... - ECIPE." https://bit.ly/2gYUfDQ Accessed 15 Nov. 2018.*
[49] *Tracing the Economic Impact of Regulations on the Free Flow of Data ...." 30 May 2016, https://bit.ly/2PujS0I Accessed 26 Oct. 2018.*
[50] *"Data Localization | Digital Import Export Trade | American Express FX ...." https://amex.co/2RVatMv Accessed 15 Nov. 2018.*
[51] *"Cloud Computing Is Crucial To The Future Of Our Societies -- Here's ...." 25 Feb. 2018, https://www.forbes.com/sites/joytan/2018/02/25/cloud-computing-is-the-foundation-of-tomorrows-intelligent-world/. Accessed 15 Nov. 2018.*

3.2 Economic Cost of Data Localisation

Perhaps the most noticeable side effect of data localization is the economic cost involved. Due to the nature of big business around the world, multinational corporations aim to consolidate their technology platforms and business operations on a regional, if not global basis. With the onset of localization, these efforts will be the first to be impacted.

Of course, the scale of the impact will differ depending on the different kinds of data on which localization is imposed and the degree of stringency attached to them. Keeping that in mind, the ECIPE developed a spectrum which gives us a better understanding of the scale to which these losses can vary.

According to the study, should the localization be carried out in specific sectors, the losses are projected to be relatively low at -0.1%. On the other end, if India were to introduce an economy-wide data localization measure, the impact would increase to -0.8%. Besides, it would also hit India's projected growth by approximately 20%. Regarding investments, exports, and long-term growth, a blanket data localization measure would result in a 1.9% drop. Losses in welfare alone could reach as high as $3.1–14.5 billion. To give perspective on what it might affect the average Indian, the adverse welfare effect would cost an Indian worker almost 11% of their average monthly salary[52].

[52] "*The costs of data localisation: friendly fire on ... - ECIPE.*" *http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf. Accessed 26 Oct. 2018.*

3.3 Increased Organisational Complexities

Data localization can significantly impact how organizations and data servers operate around the world. For instance, consider a task as simple as sending an email through Gmail. Because of the vast amount of data flows that Google has to manage, data has to be routinely shifted around in the servers owned by Google across the world. This helps maintain costs, efficiency, and scalability. However, if countries come up with stricter localization laws about emails, citing personal data as sensitive, it complicates things. Google would no longer be able to use specific data centers to share the bulk load it processes.

The report presented by Chatham House and CIGI argues that increasing organizational complexities does not fundamentally alter business economics at a country or enterprise level. Which in fact, may be right. However, it can have impacts on how companies that manage and process data as their business model operate. In other words, the complexity of dealing with data location regulations adds another challenge for managers to overcome[53].

What that could affect is the rearrangement of data servers around the world. Whole countries and regions could potentially be out of the running to host data servers for global players. This would serve as a blow to emerging economies like India who have giant IT and service sectors. The industry is still going to survive by finding cheaper alternatives elsewhere. However, it is up to India to present itself as a viable option, not only for the good of the economy but also to keep at the forefront of innovation. So at best, increased organizational complexities due to data localization can be considered a missed opportunity for a developing country like India. At worst, however, it can mean a global restructuring of where data centers will be located for years to come.

[53] "*Tracing the Economic Impact of Regulations on the Free Flow of Data ....*" *30 May. 2016, https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf. Accessed 26 Oct. 2018.*

3.4 Lower Efficiency

Talking about the global restructuring of data servers brings us to the issue of organizational efficiency on a global scale. As discussed in section 2.3, multiple factors go into deciding the physical location of data. Considering these factors allows companies to make the most efficient decision to maintain costs while maximizing the best possible experience to the end users. However, localization would bring with itself the need to retain people, infrastructure, and technology when it would make little or no financial sense.

By investing in markets that warranted no investments in the first place, organizations would be stripped off resources to invest/reinvest in areas that did warrant those investments. Moreover, it would hinder the capabilities of private actors to provide the best possible experience to their customers who may well be spread internationally. Also, data localization would have costs for efficiency because of the lack of suitable alternatives for safe data storage and processing in India. Domestic localization might mean less of a threat from foreign actors, but it would make the servers more vulnerable to domestic entities. This is not taking into account the lack of existing infrastructure to facilitate the safe storage of data as well as cooling the facility.

Localization laws on digital payments will have a disproportionate effect on domestic and international banks. For instance, international banks such as Standard Chartered or Hongkong and Shanghai Banking Corporation (HSBC) will face higher costs as compared to their domestic counterparts. The smaller scale of domestic banks will allow them to slip under the radar.

This is cause for concern not just because of the loss for efficiency and forced increase in costs, but also because of the larger implicit implication of protectionism when none is needed. If history has taught us anything about the Indian industry, it is that protectionism can be a dangerous precedent. This rings true more than ever in the age we live in today.

3.5 Reduction of the global footprint

A likely bi-product of the increased costs and lowered efficiency is the reduction of the global reach of organizations. Data location laws can not only deter but can also act as causes for organizational exit from countries. Should a private entity no longer consider costs to be worth the benefits it gets in return, operations in that country can cease to exist. The direct impact on the firm is the reduction of scope, leading to reinvesting the capital invested initially. However, the brunt of the exit might be felt on the host country, and more specifically, their citizens. Companies ceasing operations on regions can mean jobs lost for hundreds of workers. On the consumer side, it might mean the lack of options. For the industry, it might mean the exit for a competitor, for better or worse.

It is worth noting that in the case of India, it is highly unlikely for companies to consider exits. The sheer size of the market and user base compels organizations to keep on board. Besides, with the applications for big data still developing, the potential for growth in the sector is enormous. In other words, the costs are unlikely to meet the benefits. However, it is important to note that data regulations make some countries unattractive for companies. It would not be unprecedented for organizations to leave if the business does not make financial sense. Mainly because no private investors would choose to stay in a country where staying in business would require tens of millions of dollars in data center investments[54].

[54] *"Amazon opens data centers in India - The Hindu Business Line." 28 Jun. 2016, https://www.thehindubusinessline.com/info-tech/amazon-opens-data-centers-in-india/article8783403.ece. Accessed 26 Oct. 2018.*

3.6 Reduced access to financial services

While it is true that private financial institutions might not immediately leave a market as big as India because of data center costs, it does not in any means disqualify the scope of them reducing their investments. This is of particular concern when it comes to financial institutions.

India has gradually moved towards making digital and cashless payments a mainstream reality for its population. It has been cited as a rationale behind demonetization and has been the subject of numerous speeches by PM Modi[55]. For a country that desperately wants to move on from cashless payments, better financial services are a necessity. There is a tremendous scope for digitization within India's center as well as the periphery. Contactless cards and services like Apple pay are yet to penetrate the market for public services such as transport within and outside cities. There is a demand for more straightforward methods of payment. The success of alternatives to traditional banks such as PayTm, Ola Money, and Google Pay proved the same.

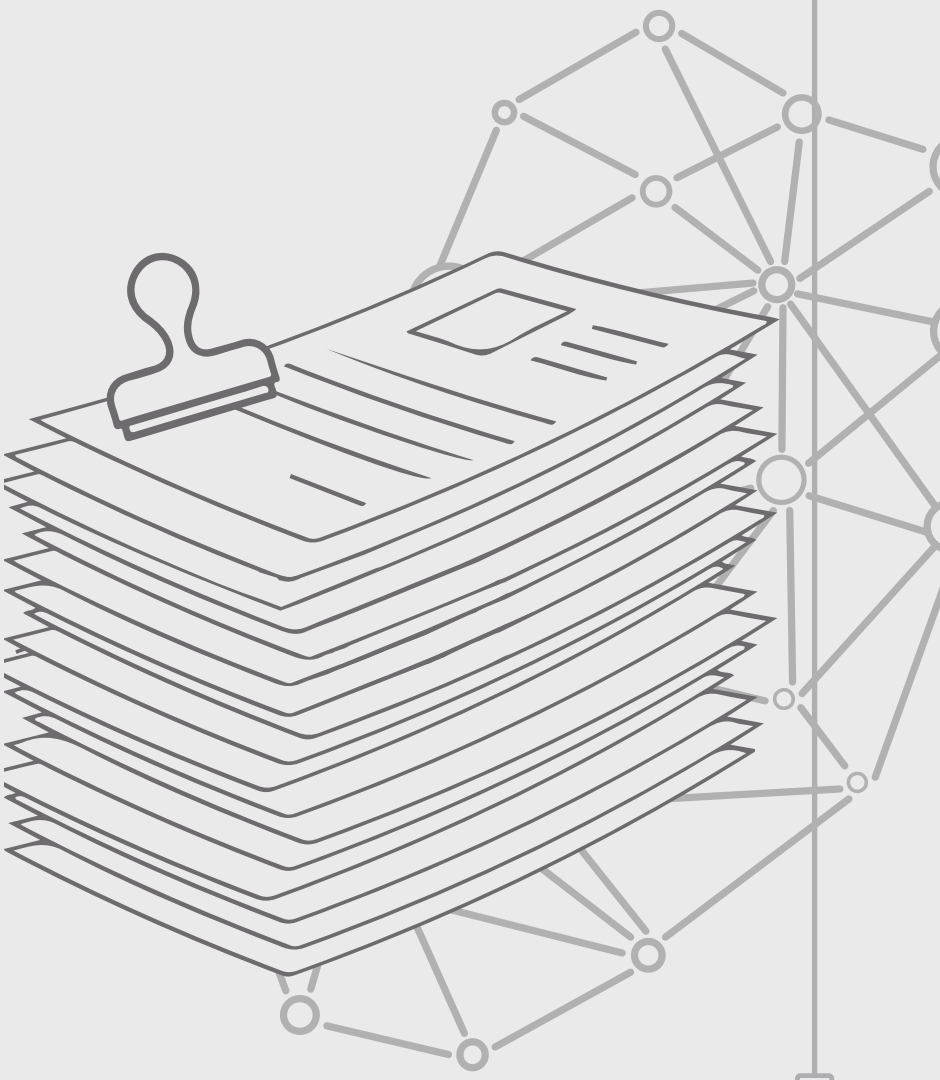
Data localization will be a step backward for the digital payments industry. Not only would it make it costlier for international banks to operate, but it would also reduce the incentive for them to innovate and try out new forms of payment on the front and back end. ‘Black money' has been a critical issue for India[56], and a push for digital and cashless transactions is a tested, long-term alternative to the same. So, in a time where better financial services can be detrimental to development, slowing down their expansion through data localization will deter the cause that the current government has been seemingly championing.

[55] *"PM Modi Defends His Decision Of Demonetisation, Says It Has Led To ...." 5 Oct. 2017, https://www.indiatimes.com/news/india/pm-modi-defends-his-decision-of-demonetisation-says-it-has-led-to-cashless-economy-331086.html. Accessed 1 Nov. 2018.*

[56] *"Black Money and Politics in India | Economic and Political Weekly - Epw." https://www.epw.in/journal/2017/7/special-articles/black-money-and-politics-india.html. Accessed 30 Oct. 2018.*

CHAPTER 4

DATA LOCALIZATION AND THE INDIAN CONTEXT



4.1 Introduction

Data localization and where India goes forward is of interest to stakeholders and neutrals around the world. The sheer size of the Indian market for data is immense. It is projected that by 2019, India will have 813.2 million mobile phone users, up from 775.5 in 2018[57]. The amount of data that will be produced and the insights that can be developed from it is a thriving proposition. This does not ring true for just private companies but the state as well. The world watching on knows that. Data could drive the optimum allocation of resources, and for an emerging India with the world's second biggest population and finite resources, that is the need of the hour. The question remains whether India is willing to accept this opportunity.

In the past three decades, India has seen tremendous technological changes. The early history of the Internet in India dates back to 1986 when it was launched as Educational Research Network (ERNET) meant only for the use of education and research purposes. It was a joint undertaking of the Department of Electronics (DOE) of the Indian Government and the United Nations Development Program (UNDP)[58]. In 2018, India now has an internet penetration of 20.26% in as of December 2017[59]. In just 30 years, technology has embedded itself in everything we do, both professional and personal front while making it more affordable.

To some extent, the more significant underlying conflict within the data localization debate is the same old struggle between the amount of jurisdiction the government should have. On the one end of the spectrum is the idea that the government should completely regulate this sector, an approach best exemplified by China. On the other end is the notion that data flows should be left to private actors, free of regulation. Regardless of where you land on the spectrum, it is going to determine the role the government will play in the sector going forward.

Since data localization is relatively new in the issue agenda cycle, different entities of the government are still finalizing an approach. There have been a few indicators of what lies in store for data localization. RBI's stance, the White Paper released by the Srikrishna Committee, the engagement of Telecom sector in localization as well as the Draft E-commerce policy, are some of the recent examples of India's adoption of this policy. This chapter will answer basic questions regarding the provisions laid out by these documents.

Scrutinizing in this paper is India's drive to push for data localization. Moreover, as of the time of writing, there have been a few significant landmarks in this journey (see Table Below). Firstly, there is the stance taken by the Reserve Bank of India (RBI). In April, RBI asked payment operators in India, including PayTM, PhonePe, and Google, to store and process data relating to the payments of Indian citizens on Indian servers. The rationale for the move was cited as facilitating the government with "unfettered access" to ensure the security of the information concerning breaches[60]. As of today, the policy is now in implementation.

[57] "*India mobile phone users 2013-2019 - Statista.*" *https://bit.ly/2i4VONn Accessed 1 Nov. 2018.*
[58] "*20 years of Internet in India: On August 15, 1995, public Internet access ....*" *15 Aug. 1995, https://bit.ly/2RZ8MOm Accessed 1 Nov. 2018.*
[59] "*Internet users in India expected to reach 500 million by June: IAMAI.*" *20 Feb. 2018, https://bit.ly/2HzAQDc Accessed 1 Nov. 2018.*
[60] "*Reserve Bank of India - Notifications.*" *6 Apr. 2018, https://bit.ly/2DmSY3L Accessed 26 Oct. 2018.*

4.2 Data Localisation in Existing Laws

The thought-process towards storing data locally has gained steam in recent times. However, there are already a few laws and provisions that expressly provide for data storage in India. Some of the essential provisions are as follows:

(i) The Companies Act, 2013

The Companies (Accounts) Rules, 2014 specified under the Companies Act, 2013 provide that a backup of the books of account and other books and papers of the company maintained in electronic mode, including at a place outside India, if any, shall be kept in servers physically located in India on a periodic basis.

(ii) The Payment and Settlement Systems Act 2007

According to Section 10(2) read with Section 18 of Payment and Settlement Systems Act 2007, the Reserve Bank of India issued a directive mandating all payment system operator to store all data relating to payment systems operated by them only in India[61].

(iii) The IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017

The Insurance Regulatory and Development Authority of India has vide the regulations as mentioned earlier mandated that all original policyholder records be required to be maintained in India.

(iv) Guidelines for Government Departments on Contractual Terms Related to Cloud Services

The Guidelines issued by the Ministry of Electronics and Information Technology, Government of India mandate all government department to include the following provision in their contract while procuring cloud services:

"The location of the data (text, audio, video, or image files, and software (including machine images), that are provided to the CSP for processing, storage or hosting by the CSP services in connection with the Department's account and any computational results that a Department or any end user derives from the foregoing through their use of the CSP's services) shall be as per the terms and conditions of the Empanelment of the Cloud Service Provider."[62]

The Guidelines as provide that the law enforcement agency as mandated under any law for the time being in force may seek access to information stored on the cloud as provided by the Service Provider. The onus shall be on the Service Provider to perform all due diligence before releasing any such information to any such law enforcement agency.

(v) The Foreign Direct Investment Policy

The Consolidated FDI Policy (as effective from August 28, 2017), issued by the Department of Industrial Policy & Promotion, also lays some requirements for keeping specific data in India for entities engaged in the broadcasting sector. Annexure 7 of the FDI Policy details the conditions required to be complied by the Indian companies engaged in broadcasting sector proposing to raise foreign investment and provides that the 'company shall not transfer the subscribers' databases to any person/place outside India unless permitted by relevant law.'[63]

(vi) The Unified License for Telecom Services

The license agreement prescribed by the

Government of India for grant of the unified license contains the following specific restriction:

"The Licensee shall not transfer the following to any person/place outside India:- a. Any accounting information relating to the subscriber (except for international roaming/billing) (Note: it does not restrict a statutorily required disclosure of financial nature); and b. User information (except about foreign subscribers using Indian Operator's network while roaming and IPLC subscribers)."[64]

(vii) The Public Records Act of 1993

The Public Records Act, 1993 deals with regulating the management, administration, and preservation of public records of the central government, union territories, public sector undertaking, etc. The said legislation prohibits transferring of public records out of India without the prior approval of the Central Government, except for official purposes.[65]

In addition to the above, the requirement to store data locally in India has been included in a few proposed policies and laws like the draft e-commerce policy, the draft e-pharmacy policy, the draft Digital Information Security in Healthcare Bill, 2017 and the proposed amendment to the Drugs and Cosmetics Rules, 1945 etc.

(viii) Draft Digital Information Security in Healthcare Act, 2018[66]

The draft Act seeks to impose data localisation concerning digital health data in India.

(ix) Data protection under the IT Act, 2000

Section 43A of the IT Act provides for the payment of compensation for failing to maintain reasonable security practices in respect of sensitive personal data. The IT Rules issued in 2011 clarified the meaning of sensitive personal data and set out the norms for the collection, disclosure, storage, and security of such information.[67]

The Table 1 in the next page depicts a sector-wise distribution of data localisation regulations in India along with the law applicable under each sector, to what types of data does the regulations apply and what are those specific restrictions and prohibitions.

[61] "*Notifications - Reserve Bank of India.*" *6 Apr. 2018, https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0. Accessed 15 Nov. 2018.*
[62] "*Guidelines for Government Departments on - MeitY.*" *31 Mar. 2017, http://meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf. Accessed 15 Nov. 2018.*
[63] "*Consolidated FDI Policy Circular of 2017 | Department of Industrial ....*" *28 Aug. 2017, http://dipp.nic.in/whats-new/consolidated-fdi-policy-circular-2017. Accessed 15 Nov. 2018.*
[64] "*Government of India - DoT.*" *http://www.dot.gov.in/sites/default/files/Amendment_UASL_1-2-06_1.pdf. Accessed 15 Nov. 2018.*

Sector	Applicability	To what types of data do the restrictions/ prohibitions apply?	What are the restrictions and prohibitions?
Telecom	1. All telecom service providers having a license under Section 4 of the Indian Telegraph Act, 1885	1. Accounting information relating to a telecom user (except for international roaming/billing related information) 2. User information	1. Storage of information outside India 2. Transfer of information to any country outside India 3. Remote access to such data from outside India
Insurance	1. All insurance companies registered with the Insurance Regulatory Development Authority of India	1. Details of all insurance policies issued by the insurers 2. Details of insurance claims made by the insured	1. Storage of information outside India 2. Transfer of information to any country outside India
Payments	1. All payment system operators who have an authorization under the Payment and Settlement Systems Act, 2007	1. Entire data relating to payment systems including the full end-to-end transaction details/ information collected/carried/ processed as part of the message/payment instruction.	1. Storage of information outside India 2. Transfer of information to any country outside India

Table 1: Sector wise distribution of data-localisation regulations in India

[65] *"The Public Records Act, 1993 | National Archives of India | Govt. of India." 11 Feb. 2018, http://nationalarchives.nic.in/content/public-records-act-1993-0. Accessed 15 Nov. 2018.*
[66] *"Digital Information Security in Healthcare Act on Cards." 28 Aug. 2018, http://innohealthmagazine.com/newscope/digital-information-security-healthcare-act/. Accessed 10 Nov. 2018.*
[67] *"India: Information Technology (Reasonable Security Practices and ...." 4 Sep. 2017, https://www.lexology.com/library/detail.aspx?g=35f56a2a-c77c-49e7-9b10-1ce085d981dd. Accessed 15 Nov. 2018.*

4.3 Justice Srikrishna Committee report and the Personal Data Protection Bill, 2018

The Justice Srikrishna-led committee report was submitted to the government on 27th July 2018. Titled, 'White Paper of the Committee of Experts on a Data Protection Framework for India,'[68] the report had some key recommendations that covered topics like jurisdiction and applicability, what it means for data fiduciaries, important data rights, and the transfer of personal data abroad.

While the report is a prelude to the bill and not final policy yet, it is one of the most reliable indicators we have on the stance India might adopt going forward. While multiple sections of the report will have indirect impacts on cross-border data flows, here is a list of impacts the report will have on the transfer of personal data abroad:[69]

1. Cross-border data transfers of personal data, other than critical personal data, will be through model contract clauses containing fundamental obligations with the transferor being liable for harms caused to the principal due to any violations committed by the transferee.[70]

2. Intra-group schemes will apply to cross-border transfers within group entities.

3. The Central Government may have the option to green-light transfers to certain jurisdictions in consultation with the DPA.

4. Personal data determined to be critical will be subject to the requirement to process only in India (there will be a prohibition against cross-border transfer for such data). The Central Government should determine categories of sensitive personal data which are critical to the nation having regard to strategic interests and enforcement requirements.

5. Personal data relating to health will, however, be permitted to be transferred for reasons of prompt action or emergency. Other such personal data may additionally be transferred by Central Government approval.

6. Other types of personal data (non-critical) will be subject to the requirement to store at least one serving copy in India.

[68] *"White Paper on Data Protection framework for India - Public ... - MeitY." 18 Dec. 2017, http://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited. Accessed 15 Nov. 2018.*
[69] *"Key Highlights From Srikrishna Committee Report on Data ... - The Quint." 27 Jul. 2018, https://www.-thequint.com/news/india/key-highlights-from-srikrishna-committee-report-on-data-protection. Accessed 26 Oct. 2018.*
[70] *"Principles Of The Evolving Data Protection Framework - Mondaq." 22 Aug. 2018, http://www.mondaq.com/india/x-/729844/data+protection/Principles+Of+The+Evolving+Data+Protection. Accessed 15 Nov. 2018.*

4.4 RBI's Localisation requirements to Financial Institutions

Before we get to examining RBI's localization requirements, it is worth mentioning the approach the bank has adopted in the past towards a digital payments infrastructure. India is still adapting to the potential of digital payments with apps such as PayTM and PhonePe. The relatively delayed onset of digital payments is partly caused by the belief that telecom companies offering cheap money-transfer services become banks first.[71] This has led to telecom companies such as Airtel roll out their services in East Africa instead. RBI's approach to online card payments is perhaps best summed up by a line in a 'Bloomberg Quint' article.

"…In 2014, the RBI required that every online card payment, even the smallest, go through a two-factor authentication process. To pay for an Uber in India, you have to enter your credit card password, swiping at your phone in the rain or blinding sun, even if your ride has cost only $1.50".[72]

So, the RBI has been skeptical of digital payments and how they shape everyday financial transactions. Moreover, when it comes to data flows, the central bank has built on this paradigm. In April 2018, RBI issued a circular requiring that all data relating to payment systems operated by system providers be stored in a system only in India within six months. The circular is not as comprehensive as the recommendations of the white paper and has a simple goal of achieving data localization as compared to the vast scope of data protection undertaken by the committee. In what is a remarkable addition to this circular, the rationale behind the move is cited as providing, 'unfettered supervisory access to data stored with these system providers, service providers, intermediaries, third party vendors and other entities in the payment ecosystem'.[73] This push for unfettered access to the data provides a sense of the government's approach to data once it is localized. The emphasis on "unfettered access" is where the challenge lies. This notion is contradictory to the principles of data protection as seeking the ownership of data lies only with the consumer and to demand unchallenged access to the same flirts with borderline surveillance.

A crucial challenge that RBI will face while implementing this policy will be around the encryption of data. Presently, RBI mandates that banks and financial institutions encrypt data onto 128 for protecting the personal data within the financial transactions. Once the transaction, its record, and the data within the same are encrypted, its access is impossible unless the relevant payment institutions break the code. It is in direct conflict with the RBI's intended approach to simplify access to data. Subsequently, does it mean that RBI is willing to compromise on the security of financial transactions with the objective to access critical information[74]? Also, in order to decrypt data, a due legal process will have to be followed.

[71] "*Why India should let its citizens' data roam free - The Economic Times.*" *14 Sep. 2018, https://bit.ly/2Dpq2bg Accessed 26 Oct. 2018.*
[72] "*India Should Let Data Roam Free - Bloomberg.*" *13 Sep. 2018, https://bloom.bg/2PY7llO Accessed 26 Oct. 2018.*
[73] "*Reserve Bank of India - Notifications.*" *6 Apr. 2018, https://bit.ly/2DmSY3L Accessed 26 Oct. 2018.*
[74] "*Data localisation in India: Questioning the means and ends - NIPFP.*" *31 Oct. 2018, https://bit.ly/2QLLScR Accessed 15 Nov. 2018.*

4.5 Data Localisation in the E-Commerce Sector

Data localization has established a precedent in the future of e-commerce in India. The Draft National Policy Framework for E-commerce was leaked earlier this year and had some new measures. Firstly, seemingly inspired China's lead of rating its citizens through a social credit system, the framework proposed for using 'Jan Dhan' account transactions to create a creditworthiness profile of individual users.[75] Secondly, the paper called to mandate RuPay as a payments terminal on each registered E-Commerce website.[76] Moreover, thirdly, it took the Srikrishna committee's suggestions on data localization and called for the same.

The draft advocates for a two year adjustment period for the industry to get used to the localization requirements. In addition to that, it also provides incentives to companies such as waivers on import duties and other taxes that they may be liable for when setting up data centers.[77] The intent is noble, but the policy lacks effectiveness. Data storage in India is an expensive affair. With the lack of available infrastructure, it would be more feasible to look for alternatives abroad. However, this scenario does not work out well for emerging startups who would have to unnecessarily pay more to avail services of relatively lower quality.

In another downside, the government will have access to the data stored by the companies in India. So getting hold of the consumer's data may be as easy as a high-level official signing a note to request access. How is such a system meant to assure customers who trust companies to keep data safe? The government has been blatant about it too, the rationale behind the move is justified by 'national security and public policy objectives.' So, in the event of such an approach being adopted, there should be a call to develop standards for access to data. It would go a long way in setting the right example for an economy that needs E-commerce to prosper for its success.

Should these clauses in the draft be approved and made into law, they will serve as obstructions to the growing e-commerce industry in India. According to the India Brand Equity Foundation, the e-commerce segment in India is projected to grow to a $200 bn market in the next eight years.[78] Also, it is not just India that E-commerce will expand in, giants such as Amazon, Alibaba, and Walmart will use data flows to advance their sectors over the years. Also, while the rest of the world partakes in this exercise, the role India wants to undertake is up to her. She can either lead the cause and be at the forefront of the progress or go through with data localization and oppose promising sectors like e-commerce.

[75] *"Draft National E-commerce Policy: data localization and priority to ...." 7 Aug. 2018, https://www.medianama.com/2018/08/223-draft-national-e-commerce-policy-data-localization-and-priority-to-domestic-companies/. Accessed 26 Oct. 2018.*

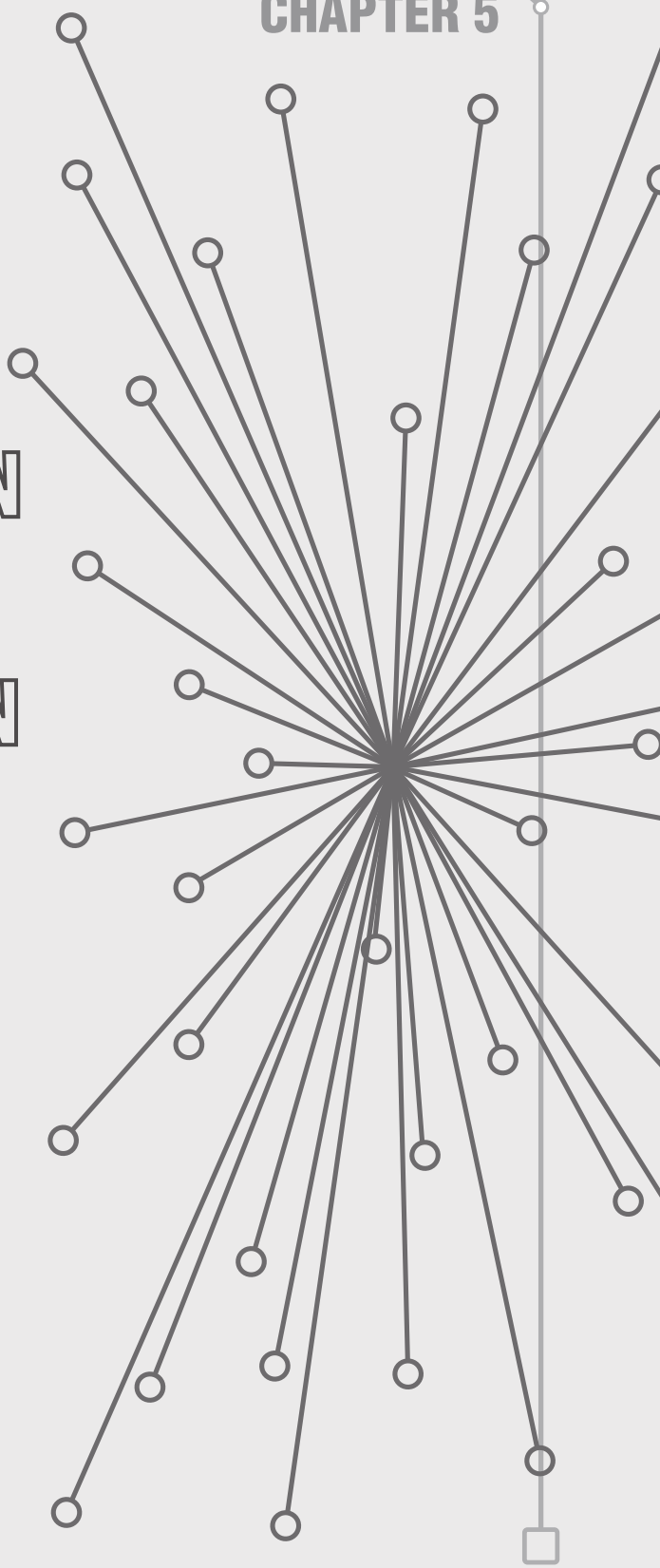
[76] *"Electronic Commerce in India: Draft National Policy ... - MediaNama." https://www.medianama.com/wp-content/uploads/Draft-National-E-commerce-Policy.pdf. Accessed 26 Oct. 2018.*

[77] *"Electronic Commerce in India: Draft National Policy ... - MediaNama." https://www.medianama.com/wp-content/uploads/Draft-National-E-commerce-Policy.pdf. Accessed 26 Oct. 2018.*

[78] *"E-commerce in India: Industry Overview, Market Size & Growth| IBEF." https://www.ibef.org/industry/ecommerce.aspx. Accessed 26 Oct. 2018.*

CHAPTER 5

ANALYSING THE MOTIVATION BEHIND DATA LOCALIZATION IN INDIA



5.1 Introduction

Data localization is a complex subject. Regardless of what the government's approach is, the content of the white paper and the overall output that followed makes it evident that the parties leading the debate are well versed with the sector. This begs the question of why the paper adopted the stance it did. The recommendations of the white paper do not call for data localization in isolation. In advocating for a localization measure, the white paper is joined by the RBI (through its circular for Storage of Payment System Data) as well as the Draft National E-commerce policy.

The proposition made by proponents of localization is that there will be benefits for local industry participants. This proposition appears to flow almost directly from the infrastructure and skill-related gains that seem to flow to Indian territory and personnel. It is believed that both domestic and foreign players may be involved in the creation of these and since the storage would be in India, any processing and analysis of the same would also have to happen here.

It seems that market entry barriers created would in all likeliness only foreclose the smallest players (bigger ones being able to afford the costs) and the effect would thus not be like other protectionist measures. Whether these benefits outweigh the considerable costs that emerge (entrenchment of big players, reduction in levels of competition, etc) is something that this chapter will try to identify and answer.

In order to better understand the motivation behind the push for data localization, it is imperative to analyze the scenario from the government's perspective. The chapter will explore recurrent themes within the government's narrative and identify whether data localization fits in as a solution. This will include arguments such as national security, law enforcement, the growth of the IT sector, and financial implications. The chapter will then critically evaluate these claims to test their validity. This will help separate myths from facts, making for more informed dialogue on the subject.

5.2 National Security and Law Enforcement

Perhaps the government's most persuasive case for data localization has to do with the argument of national security. It is a constant theme in the policy proposals that have released thus far. The White Paper itself dedicates a section to the same with the title, 'National security or security of State and other similar grounds.' The crux of the argument is laid out in the section's first paragraph:

"….the State may have an interest in placing reasonable limits on informational privacy in the interest of national security, security of (the) state and other similar grounds. Other grounds could include objectives such as upholding the sovereignty and integrity of India, maintaining friendly relations with foreign states, maintenance of public order and preventing incitement to the commission of offenses".[79]

There is a case to be made in favor of the argument that the state should have access to personal data. The role of hate speech on Facebook in Myanmar's Rohingya crisis serves as a reminder today.[80] Apart from hate speech, cyberspace is littered with what some would call fake news, and can also potentially serve as a platform to mobilize against the state.

While 'traditional data' may be insufficient to keep track of these instances, cyber data is the best available tool to achieve these ends. Private companies with their cloud servers are hesitant to let the government access to their consumer data. This was made clear on an international forum when Apple Inc. refused to aid the FBI in unlocking the iPhone used by Syed Rizwan Farook in the December mass shooting in San Bernardino, Calif.[81] Keeping this in mind, it is understandable that data localization may appear as a viable solution to India's growing vulnerability in the cyberspace.

On a related note, data localization is also supposed to aid in the more effective functioning of law enforcement agencies. The White Paper mentions the same in 9.2 (iii), a section titled, 'Easy Access of Data in Support of Law Enforcement and National Security.' The paper argues that regarding when law enforcement agencies enforce jurisdictional claims against foreign entities through Mutual Legal Assistance Treaties (MLATs). MLATs are agreements among two or more nations regarding collecting and sharing information for effective law enforcement.

Data confidentiality is the essence of the policy debate around data localisation. It appears that data confidentiality is driven by the need to store sensitive data at captive data centers or through other vendors who either provide platform or services of cloud storage or as the case may be. These data centers and vendors are regulated by various industry verticals, standards, and legal compliances. The argument goes that should the data servers be put in India, the law enforcement agencies will have access to a larger pool of data. This is opposed to a situation where the servers are hosted abroad, and foreign sovereign powers can deny access to data. Thus, localization will be conducive to the interests of Indian law enforcement.

Will it help in access?

However, merely hosting data in a particular jurisdiction does not increase the lawful access of such jurisdiction to such data, primarily due to conflict of laws from jurisdictions in which parent organization that may have custody, ownership, and control over such data are registered, the location of encryption keys, etc.

Further, it is well documented that even currently, access to data for lawful/legitimate purposes is enabled and made possible without a requirement of the physical location of data. In the cloud era, countries that honor baseline principles of privacy, human rights, and due process should be able to efficiently access data (irrespective of where it is stored) that pertains to severe crimes that happen within their borders and users who are within their jurisdiction.

Because of the provisions of the Personal Data Protection Bill regarding jurisdiction and applicability, it is believed that the provisions of Indian law should apply to access to personal data stored (processed) in India. It is however not so straightforward. Since the data has been processed by a foreign company, which may be subject to the laws of the country where it is incorporated, there may be an inevitable conflict of laws situations. In order to minimise and avoid potential conflicts, while legislating in domestic laws, it needs to be kept in mind that domestic laws relating to privacy and data protection comply with established principles of international law. Later in the study, the author(s) identify alternate and more progressive means to help law enforcement agencies access data from foreign companies.

Additionally, the recent Supreme Court judgement[82] on Aadhaar (Targeted Delivery of Financial Benefits and Other Subsidies, Benefits, and Services) Act, 2016 struck down Section 33(2), that mandated "unfettered access" to people's data.

Access to data is now not permitted automatically even is sought for national security purposes. This sends a powerful message by the highest judicial body that in cases where the state is seeking access to data there has to be a due process of law and high-level safeguards in place to prevent the potential misuse of such data. This judgement, therefore, has identified a precedent that the state should follow concerning placing enough checks and balances before data is sought to be accessed.

[79] "*WHITE PAPER OF THE COMMITTEE OF EXPERTS ON A ... - MeitY.*" *4 Nov. 2017, http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf. Accessed 31 Oct. 2018.*

[80] "*Revealed: Facebook hate speech exploded in Myanmar during ....*" *3 Apr. 2018, https://www.theguardian.com/world/2018/apr/03/revealed-facebook-hate-speech-exploded-in-myanmar-during-rohingya-crisis. Accessed 31 Oct. 2018.*

[81] "*Apple opposes order to hack gunman's phone - CNN - CNN.com.*" *18 Feb. 2016, https://www.cnn.com/2016/02/16/us/san-bernardino-shooter-phone-apple/index.html. Accessed 31 Oct. 2018.*

[82] *Justice K.S. Puttaswamy (Retd.) and Ors. Versus Union Of India And Ors. (W.P.(C) 494/2012)*

5.3 Data Security

Data localization is also considered a step towards national security because of how it can act as a barrier to prevent foreign surveillance and illegal data breaches. If data servers with critical personal servers were stored abroad, it is feared that it would allow foreign governments to impinge upon the privacy and security of the data of indoor nationals.

Issues involving cybersecurity, or the protection of data from unauthorized access by others—whether rogue individuals or other governments, is a legitimate concern. The rise of cyber terrorism and cyber espionage by governments has heightened the concern for the security of data stored outside a country's borders.

5.3.1 Single Point Concentration of Data makes it More Vulnerable

Data does not become secure when placed at a single location. Instead, it becomes more vulnerable. Protecting data from risk is not necessarily about eliminating the element of risk. In a more pragmatic sense, it is a trade-off between managing risk while maximizing the opportunities of connectivity and data flows. As the OECD has recommended, the treatment of digital risks "should aim to reduce the risk to an acceptable level relative to the economic and social benefits expected from these activities".[83]

The ability to implement and maintain robust data storage processes, provide controlled access to data, streamlined processes for operational efficiency, meeting global cybersecurity standards and much more are required to secure data. Merely dictating the location of where the data is stored does not work towards the goal of data protection and security. Cyber attacks are global, physically location the servers in India does not protect the data from attacks or damage from disasters.

Security is not enhanced just because data resides within a particular jurisdiction. Security is a function of the technical, organizational, and financial capacity of an entity to protect the data and provide physical protection for a data center.[84]

So instead of storing data in centers around India, security would be better facilitated with the creation and use of de-centralized and end-to-end encrypted services that do not store all consumer data in one place.

5.3.2 Centralized Systems

Governments risk security when they require data to be centralized domestically. This leads to a single point of attack which can be avoided by using cutting-edge cloud data centers that, for example, might share data globally and regularly backup copies of data across globally located data centers. Centralizing information about users in a locality might ease the logistical burdens of foreign intelligence agencies, which can now concentrate their surveillance of a particular nation's citizens more efficiently.[85]

5.3.3 Foreign Surveillance Possible with Locally Stored Data

Data centers located in India will need to be subject to stringent standards and demonstrate their ability to protect our data –

through cybersecurity and physical security measures, not just from criminals, but also unwarranted government surveillance. Data centers without a large amount of uninterrupted power supply, cooling facilities and cybersecurity measures implemented can also corrupt, destroy or damage Indian data.

[83] "*Digital Security Risk Management for Economic and ... - OECD.org.*" *17 Sep. 2015, https://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf. Accessed 30 Oct. 2018.*
[84] "*Data Processing and Security Terms | Google Cloud Platform Terms ....*" *7 Feb. 2017, https://cloud.google.com/terms/data-processing-terms-20170207. Accessed 30 Oct. 2018.*
[85] "*data nationalism - Emory Law.*" *19 Feb. 2015, http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf. Accessed 11 Nov. 2018.*

5.4 Does Data Localization Equals Ownership of Data?

Another critical aspect thought by the govt to legitimize localization is based on the concept of data ownership. It is defined only as "the act of having legal rights and complete control over a single piece or set of data elements. It defines and provides information about the rightful owner of data assets and the acquisition, use and distribution policy implemented by the data owner".[86]

In simpler terms, the idea of data ownership is fundamental to the role of data in our lives. What is the purpose of using data? Moreover, who deals with it? These are some of the challenging questions that are addressed by this concept. In an ideal world, the user, we the people, own our data. In a truly democratic fashion, the idea of data itself is based on freedom. The freedom that emancipates from the choice to use the internet to connect with friends and family, to go about one's daily routine, sharing ideas with the world and interacting with one another. It is the only place on earth that doesn't have borders. The freedom to control your information is the ticket to unhinged consumption of the internet that has become such an intrinsic part of our lives and how we go about doing our things.

While the consumer owns the data, the power to derive insights based on such data and monetise the same is something that fascinates businesses and governments alike. Governments across the world are attempting to drive insights that could help in delivering better services to their people and

5.4.1 Data is the New Oil

The most popular argument concerning data in the public domain is the ‘oil' argument. Data is globally regarded as the next best commodity for oil. The notion is that whoever controls the data, controls power. Experts and leaders across the world have increasingly begun to recognize the power of data. This is why the issue of data is not just a matter of technology, it is now a leading domestic policy matter (with enormous geopolitical and strategic implications) that sovereign nations aspire to get right. The power of data resides in its commercial exploitation and strategic advantage. It can bring fundamental changes to democratic setups and drive long-term impact. Industries such as healthcare, infrastructure, agriculture, etc are already witnessing the impact of data. Insights and analytics that are generated by controlling and processing data can shape the future of the world. Therefore, it is not surprising that governments are vying to control the flow of data. India is a significant global player that is surging ahead with a growing internet base. With the fast-paced growth in the number of internet users, businesses can innovate significantly in technology and overtake their competition. Indeed, foreign businesses would like to compete with their counterparts for the long-term goal of impacting nearly a billion users with their products and services.

While analytics promises excellent economic growth, the strategic advantage of data trumps everything else. Geospatial and satellite enabled technologies are at the core of monitoring of adversarial activities driven by non-state actors. Internal security can be significantly enhanced with the smart deployment of data analytics tools. Like corporates, governments also collect and

process data to defend the borders and safeguard the privacy and security of its citizens. Instead of ensuring free movement of information, one cannot forget the criticalities that revolve around data's national importance.

Will storage help in increasing India's analytics footprint and bringing home strategic advantage? This is an incorrect question to ask, as the argument does not fit a binary response. However, for the sake of our research and looking at the current state of affairs, the answer is in negative. To realize the dream of 'data is the new oil' and to maximize national security potential, where data is stored does not matter.

This is because of the following reasons:

• Securing Privacy: Any perspective that believes that storage means 'easy' access is a self-contradicting notion. For any access to data, governments have to comply with a due process of law, mandated by the local privacy laws. Mere storage will not guarantee access because even if the data is stored domestically, user privacy must be protected under data protection laws, which is the same for data stored abroad. This is precisely the case with India, which is going to enact a privacy law very soon.

• Processing is key to Analytics: The power to process is fundamental to drive analytics for commercial and strategic gains. Storage has nothing to do with the power of processing. Just because the data may be stored in India, it does not mean that Indian tech companies will get access to do analytics on it.

• Access does not depend on storage: Access to data for law enforcement has little to do with the physical location of data. Indeed, its essential from a security standpoint, but in order to satisfy the domestic legal obligation, storage is not the critical aspect. The depth of bilateral, domestic privacy regimes and the internet freedom index are the real leverage points for accessing data for law enforcement. Enforced storage will only deter companies and threaten to create an unwarranted rift between companies and governments. From a strategic perspective, the real ownership does not reside with that jurisdiction that stores data, but the jurisdiction that mandates processing. For India to realize this potential, the government should invest in developing local talent that can provide services akin to what American and European companies are, at similar quality levels.

• Later in the study, we identify the right policy mechanisms that could support India to truly exploit the potential of data analytics and insight.

[86] "*What is Data Ownership? - Definition from Techopedia.*"
https://www.techopedia.com/definition/29059/data-ownership. Accessed 4 Nov. 2018.

5.5 Growth of The IT Sector and Financial Security

The Srikrishna Committee report acknowledges the potential IT and AI have to fuel progress in the economy. Being a fundamental cause for economic growth, AI has the potential to add 1.6 % to China's GDP by 2035.[87] In a similar vein, the growth of AI is expected to contribute massively to India's economy by adding 1.3% to the GDP by the same time.[88]

The growth of AI is mostly dependent on harnessing data and its capabilities. The report claims that this serves as precedence to keep data servers in India to store and process data in the country by local infrastructure. Keeping servers in India is expected to drive foreign direct investment in digital infrastructure. Besides, the presence of servers in India will be conducive to the development of the digital industry through the 'enhanced connectivity' and the presence of skilled professionals. The section cites this as rationale enough to at least keep a copy of personal data stored in India.

However, the assumption that data localisation will drive AI growth is mistaken. Every day, large amounts of data flows course through the internet, over borders and between individuals, firms and governments to power technologies and drive growth.[89] A significant portion of these data flows are used to fuel AI applications such as Siri, Waze and Google searches. Because many of these data flows are directly or indirectly associated with a commercial transaction, they are essentially traded. AI applications, "which use computational analysis of data to uncover patterns and draw inferences, depend on machine learning technologies that must ingest huge volumes of data, most often from a wide variety of sources".[90]

According to Susan Ariel Aaronson, senior fellow with the Global Economy Program, when it comes to trade laws, a massive amount of data flows over borders to power AI — but the rules are yet to be finalised.[91]

In addition to facilitating the growth of the IT sector, the report believes data localization is also conducive to financial security. Financial services are one of the building blocks of the economy. Moreover, as of recent years, India has been pushing for significant reform in the sector. Specifically, there has been a widespread call for India to be a cashless economy. Moreover, while going cashless will be beneficial for the nation, it requires the rapid building of a safe and secure digital payments infrastructure to facilitate this change at the back end. In doing so, India can:

a) Survive hostile attacks by foreign state & non-state actors alike.
b) Insulate our payment systems against foreign sanctions and politics.

The primary driver to achieve these goals is the RBI. To ensure a safe transition to a cashless economy, the central bank has opted for a path of financial prudence. To that extent, it makes for a perfect rationale for the RBI to require payment companies doing business in India, to process and store consumer's transaction data within the domestic borders. This mandate forces all stakeholders to be compliant with Indian laws and minimizes the overall exposure of our payment services getting crippled due to external events.

5.5.1 LOCALIZATION IS NOT CAUSAL FOR ECONOMIC GROWTH

The narrative that localization enhances growth is likely mistaken. Current policies and recommendations are backed with the desire to attract investment, fuel innovation and create a competitive advantage for local companies. However, it is common knowledge the impact localization and protectionism can have on the industry. Multiple factors enable the industry to grow such as tax cuts, conducive business environment, high-speed bandwidth ecological stability. Many countries have adopted the latter and then moved to legislative compulsion at a time where competitive advantage seized to be the deciding factor. Mandating localization in silos will result in unsustainable and disparate growth.

The consultation paper on data protection released by the Justice Srikrishna Committee details the same with the impact of data localization in seven countries, based on a recent research study. It found that the impact of data localization legislations on GDP was substantial in seven countries: Brazil (-0.8%), China (-1.1%), EU (-0.4%), India (-0.8%), Indonesia (-0.7%), Korea (-1.1%) and Vietnam (-1.7%) . The study also quantified welfare losses in these economies including the impact on domestic investments. For India, the loss per worker is equivalent to 11% of the average monthly salary, about 13% in China and around 20% in Korea and Brazil.[93]

So, localization will ensure that the IT sector will be less competitive, making business more comfortable for them. Besides, while it is critical that financial stability be ensured for India, it is important to realize that innovation and security more often than not, exist in a state of trade-off.

Also, what might go unnoticed when looking at domestic giants, is that localization will severely affect the growth of the local SMEs, growing e-commerce startup ecosystem, and the country's ease of doing business reforms. It would make it tougher for Indian startups and MSMEs to compete effectively in the global marketplace. India currently boasts of the 3rd largest base of startups in the world while MSMEs contribute approximately 37.5% of India's GDP.[94]

Today, all traditional industries use data analytics to enhance process efficiency, sales, and profitability. The rapid adoption of technology has placed data as an essential input in business and commerce. One of the many positive effects of global data flows, and the growth of digital platforms is that it has become easier for small and medium enterprises across all countries to participate in the global economy. Data localization could force firms offering services such as cloud computing technologies to either stop serving Indian customers or relocate all data relating to Indian users to data centers in India. Should increased costs because of the latter, trickle down to the consumer, they might be forced to decide between cheaper domestic options or world class expensive options. Rising costs in cloud computing would divert resources away from investments in quality and innovation. This would be a difficult choice to make for aspiring start-ups. Such outcomes are inconsistent with the spirit of the government's Digital India initiative.

Cloud computing based services are affordable for consumers and small businesses/startups because they rely on massive economies of scale with globally distributed data centers. Requiring data centers to be located domestically dramatically undermines the cost-effectiveness of cloud-based computing services and reduces the choices available to India's homegrown technology sector.

MSMEs should have an option on whether to use domestic cloud service providers or foreign providers depending on the quality of services and competitiveness of the cost. Otherwise, Indian MSMEs will suffer from the disadvantage of losing access to globally available cloud resources while MSMEs in other countries will enjoy the benefits of adequate cloud infrastructures as well as significant transborder investments. Data localization will also place significant pressure on the government from a technical, financial and regulatory environment perspective to create local infrastructure for smaller players. The following illustrates the role played by cross-border flows of data in empowering startups and MSMEs in India - According to a McKinsey report, 80% of tech-based startups worldwide are "born global"utilizing foreign customers, financing, suppliers from day one.[95] In a global startup survey, 86% of respondents pointed to at least one cross-border activity. Almost two-thirds have customers or users in other countries, and almost half reported sourcing workforce resources from other countries.

Enforcing restrictions on cross-border flows will hinder the ability of India startups to compete with their global counterparts due to different increased costs and compliance burdens they will have to undertake, unlike their global counterparts. These restrictions will also reduce the inflow of foreign investment such startups bring to India by reducing their attractiveness to investors. Further, it is estimated that there are around 51 million MSMEs in India which contribute 37.5% to India's GDP.[96] 68% of the 51 million MSMEs operate offline in India today. According to a KPMG report, the digitization of MSMEs could help increase their contribution to India's GDP by ten percentage points, taking it up to 46-48% by 2020. Affordable cloud-based online tools are already helping Indian MSMEs drive their exports and cross-border data flows are fundamental to this development.[97]

It is estimated that cutting off access to global cloud computing services— through localization— would force local companies in Brazil and the EU to pay 10.5 to 62.5 percent more for some cloud computing services[98]. According to the World Bank and OECD, about 43 percent of Indian export-oriented MSMEs depend on online tools for 75 percent of their global sales. Mandating data localization provisions will drive up the costs incurred by MSMEs in utilizing digital tools, reduce their odds at effectively competing with their global counterparts and lockout free access to global markets. Finally, according to a Fifth Era report, 81 percent of investors who responded to a survey for the report said they are uncomfortable investing in internet business in India if the enterprises are obligated to store user data on servers located in India and build their own data centers locally.[99]

India's net exports from its IT sector accounted for over the U.S. $116 billion in the previous fiscal year[100]. Meanwhile, India's big data analytics sector in India is expected to witness an eight-fold growth to reach $16 billion by 2025[101]. This inflow, largely based on free-flowing data, would be severely restricted by requiring data localization from all players wishing to offer services in and from India. According to a BIF-ICRIER report, it is estimated that mobile apps, which are overwhelmingly hosted outside India, contributed a minimum of USD 20.4 billion in 2015-16 to India's GDP, and this contribution is expected to grow to USD 270.9 billion by 2020.[102] This would be nearly 8% of India's GDP. The study also finds that while a 10% increase in total free-flowing Internet traffic and mobile Internet traffic globally increases global GDP by 1.3% and 0.7% respectively, for India the impact is much higher[103]. In India, a 10% increase in free-flowing total Internet traffic,

delivers on average a 3.3% increase in India's GDP[104]. Enforcing data localization requirements on app developers, which are mostly individuals or startups, would massively reduce this substantial economic impact due to increased compliance costs. This would also have a chilling effect on domestic bootstrapped innovation by imposing a high barrier of entry for new local entrants in a wide range of sectors in the Indian market.

Free flow of data in an inherently connected world appears essential to macroeconomic growth and development. Particularly for India, cross-border data flows have been critical for the establishment and growth of its outsourcing sector. India's IT-BPM industry, which has been founded on the global free flow of data, accounts for 55% of the world's outsourcing market and is worth US$ 173-178 billion[105]. The IT-BPM industry has a share of 45% in India's total service exports and contributes ~7.7% to India's GDP[106]. This industry also employs a workforce of approximately 10 million workers in India. Actions to restrict cross-border data flows will seem duplicitous on India's part due to the benefits it has reaped from such flows in the past. Such actions will therefore directly lead to a reduction in India's standing on the world stage which could harm growth, reducing

[87] "*how artificial - Accenture.*" *30 Jun. 2017, https://www.accenture.com/t20170629T190038Z__w__/cn-en/_acnmedia/PDF-55/Accenture-How-Artificial-Intelligence-Can-Drive-Chinas-Growth.pdf. Accessed 31 Oct. 2018.*

[88] "*Artificial Intelligence Could Add $957 Billion to Indian Economy ....*" *21 Dec. 2017, https://newsroom.accenture.com/news/artificial-intelligence-could-add-957-billion-to-indian-economy-according-to-new-research-by-accenture.htm. Accessed 31 Oct. 2018.*

[89] "*1.2 Cross-Border Data Flows, Digital Innovation, and Economic ....*" *http://reports.weforum.org/global-information-technology-report-2016/1-2-cross-border-data-flows-digital-innovation-and-economic-growth/. Accessed 15 Nov. 2018.*

[90] "*Data Minefield? How AI is Prodding Governments to Rethink Trade in ....*" *3 Apr. 2018, https://www.bsa.org/news-and-events/bsa-in-the-news/2018/april/en-04032018-data-minefield-how-ai-is-prodding-governments-to-rethink-trade-in-data/?sc_lang=en. Accessed 15 Nov. 2018.*

[91] "*Susan Ariel Aaronson | Centre for International Governance Innovation.*" *https://www.cigionline.org/person/susan-ariel-aaronson. Accessed 15 Nov. 2018.*

[92] "*The Costs of Data Localisation: A Friendly Fire on Economic ... - ECIPE.*" *15 May. 2014, http://ecipe.org/publications/dataloc/. Accessed 31 Oct. 2018.*

[93] "*The Flow Of Data Across Borders - USCIB.*" *https://www.uscib.org/uscib-content/uploads/2016/03/2016_03_The-Flow-of-Data-Across-Borders_A-BIAC-Trade-Committee-Policy-Pe....pdf. Accessed 31 Oct. 2018.*

[94] "*The new wave Indian MSME-An action agenda for growth - KPMG.*" *https://assets.kpmg.com/content/dam/kpmg/pdf/2016/03/The-new-wave-Indian-MSME.pdf. Accessed 5 Nov. 2018.*

[95] "*digital globalization: the new era of global flows - McKinsey & Company.*" *https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx. Accessed 5 Nov. 2018.*

[96] "*Most powerful engine of India's growth: Service MSMEs - The ....*" *27 Jan. 2018, https://economictimes.indiatimes.com/small-biz/sme-sector/most-powerful-engine-of-indias-growth-service-msmes/articleshow/62670137.cms. Accessed 5 Nov. 2018.*

[97] "*Impact of e-commerce on SMEs in India - KPMG.*" *https://assets.kpmg.com/content/dam/kpmg/pdf/2015/10/Snapdeal-Report_-Impact-of-e-Commerce-on-I*

available jobs and hamper foreign investment. Given India's rapid development, these hard-hitting statistics are bound only to have increased over the past few years. All of this data showcases the integral value that cross-border data flows have created for the Indian economy. Any hindrances to such cross-border data flows would adversely impact innovation, economic competitiveness, foreign investment and availability of affordable technology to users across the country.

ndian-SMEs.pdf. Accessed 5 Nov. 2018.

[98]"*Strong Winds Ahead for Cloud Computing: Can Data Localization ....*" *29 Apr. 2016, https://www.rand.org/blog/2016/04/strong-winds-ahead-for-cloud-computing-can-data-localization.html. Accessed 5 Nov. 2018.*

[99]*Primary Inputs*

[100]"*IT export growth to be lower in 2017-18 at 7-8pc: Nasscom - YourStory.*" *23 Jun. 2017, https://yourstory.com/2017/06/it-export-growth-lower-nasscom/. Accessed 31 Oct. 2018.*

[101]"*Big data analytics to reach $16 billion industry by 2025: Nasscom, IT ....*" *23 Jun. 2016, https://cio.economictimes.indiatimes.com/news/big-data/big-data-analytics-to-reach-16-billion-industry-by-2025-nasscom/52885901. Accessed 31 Oct. 2018.*

[102]"*BIF Recommendations for NTP on New Technologies - Broadband India ....*" *https://www.broadbandindiaforum.com/images/national-telecom-policy-2018/BIF-Recommendations-on-New-Technologies.docx. Accessed 5 Nov. 2018.*

[103]"*BIF Recommendations for NTP on New Technologies - Broadband India ....*" *https://www.broadbandindiaforum.com/images/national-telecom-policy-2018/BIF-Recommendations-on-New-Technologies.docx. Accessed 5 Nov. 2018*

[104]"*BIF Recommendations for NTP on New Technologies - Broadband India ....*" *https://www.broadbandindiaforum.com/images/national-telecom-policy-2018/BIF-Recommendations-on-New-Technologies.docx. Accessed 5 Nov. 2018*

[105]"*to Download File - IBEF.*" *https://www.ibef.org/download/IT-_ITeS-Report-Apr-20181.pdf. Accessed 5 Nov. 2018.*

[106]" *Indian IT-BPM industry GDP share 2009-2017 | Statistic.*" *https://www.statista.com/statistics/320776/contribution-of-indian-it-industry-to-india-s-gdp/. Accessed 31 Oct. 2018.*

5.6 Avoiding Reliance on Undersea Cables

According to the White Paper, a suitable rationale to shift towards data localization is to reduce the dependence on undersea cables. The location of most of the undersea cables in the world is publicly accessible. This renders them significantly vulnerable to attack. Such a scenario would significantly hinder India's communication capabilities. Data localization would serve as a measure to prepare for the same. The risk of data sabotage from undersea cable flow is part of the justification for localization provided by the Srikrishna Committee that submitted a Data Protection report to MeiTY.

5.6.1 There are Easier Methods to Damage Data Flows

There has been much said about this particular rationale stated in the Srikrishna committee report. An attack on undersea fibre cables sounds preposterous and might never become a reality. However, that is no reason to disqualify this rationale.

Destruction and tampering with data do not solely depend on a continent-scale event. There are much easier ways to achieve the same and the vulnerabilities in domestically placed servers would be exponentially easier to target than a cable lying at the seabed.

For instance, a study by the Leviathan Security Group stated that in 2011, data was compromised because of a slow water drip in a nondescript office building in Calgary, Alberta. The lack of adequate infrastructure set off an explosion that caused days of computer outages for hospitals, ambulances, radio stations, taxis, and criminal justice facilities around the province.[107]

Vying for reducing dependencies on undersea cables also goes against the very principal the undersea cables and the internet stand for. Installing border controls on the transmission of data splinters the internet, the core of which is interconnectedness into several clusters of networks. This balkanization of the net weakens the data security measures considerably.[108]

There is currently no global framework in place that prevents disconnection of a country from the Internet. Localisation would not solve the problem of disconnection from the broader Internet. Any online data transfer has the risk of being surveilled - whether this is using undersea cables or another mechanism such as satellites.

At present, satellite communication only carries less than 1% of our global internet traffic.[109] The rest of all communication relies on the intricate undersea cable network that crisscrosses all across our ocean floor. Satellite communication cannot carry the data load that is required to sustain our data requirements.

The National Digital Communications Policy[110] promotes broadband access and connectivity for all Indians, laying of optical fibre cable networks and improving satellite communications to promote the Digital India Mission. India has nearly 500 million internet users[111] – Moreover, this number is growing by the minute. According to a Nielsen survey, while Indian customers used to consume 4GB of data a month, we now consume 1GB of data a day.[112] If our plans to introduce 5G and advance the Internet of Things (IoT) technology in this country are successful, the amount of data generated and consumed is only going to increase.

India will have to join hands with the UK, the United States and other countries in addressing the issue of tapping undersea cable communication or preventing cable sabotage or damage including increasing navy surveillance of the cables and other measures. In this digital age, it will be virtually impossible to prevent data flows across-borders since a country's economic growth is increasingly tied to this flow.[113]

[107] *"The Harms of Forced Data Localization — Leviathan Security." 25 Feb. 2015, https://www.leviathansecurity.com/blog/the-harms-of-forced-data-localization. Accessed 31 Oct. 2018.*
[108] *"The Debate – Data Localization And Its Efficacy - Data Protection - India." 17 Sep. 2018, http://www.mondaq.com/india/x/736934/Data+Protection+Privacy/The+Debate+Data+Localization+And+Its+Efficacy. Accessed 31 Oct. 2018.*
[109] *"In Our Wi-Fi World, the Internet Still Depends on Undersea Cables." 3 Nov. 2015, http://www.govtech.com/network/In-Our-Wi-Fi-World-the-Internet-Still-Depends-on-Undersea-Cables.html. Accessed 5 Nov. 2018.*
[110] *"National Digital Communications Policy-2018 | Department of ...." http://www.dot.gov.in/whatsnew/national-digital-communications-policy-2018. Accessed 15 Nov. 2018.*
[111] *"Number of Indian internet users will reach 500 million ... - Times of India." 20 Feb. 2018, https://timesofindia.indiatimes.com/business/india-business/-number-indian-internet-users-will-reach-500-million-by-june-2018-iamai-says/articleshow/62998642.cms. Accessed 5 Nov. 2018.*
[112] *"Indians on an average consume 1GB data a day on smartphones ...." 27 Sep. 2018, https://www.indiatvnews.com/technology/news-indians-on-an-average-consume-1gb-data-a-day-on-smartphones-466020. Accessed 31 Oct. 2018.*
[113] *Primary Input*

5.7 Digital Tax

Another key argument that has been proposed by the Government rests around taxing foreign companies on the income generated through ad-revenue through data processed of Indian citizens.

This is supported by the view that hosting of local servers in the territory of a country would make it possible to assert the existence of a 'fixed place of business,' hence attracting taxation provisions under becoming a permanent establishment.

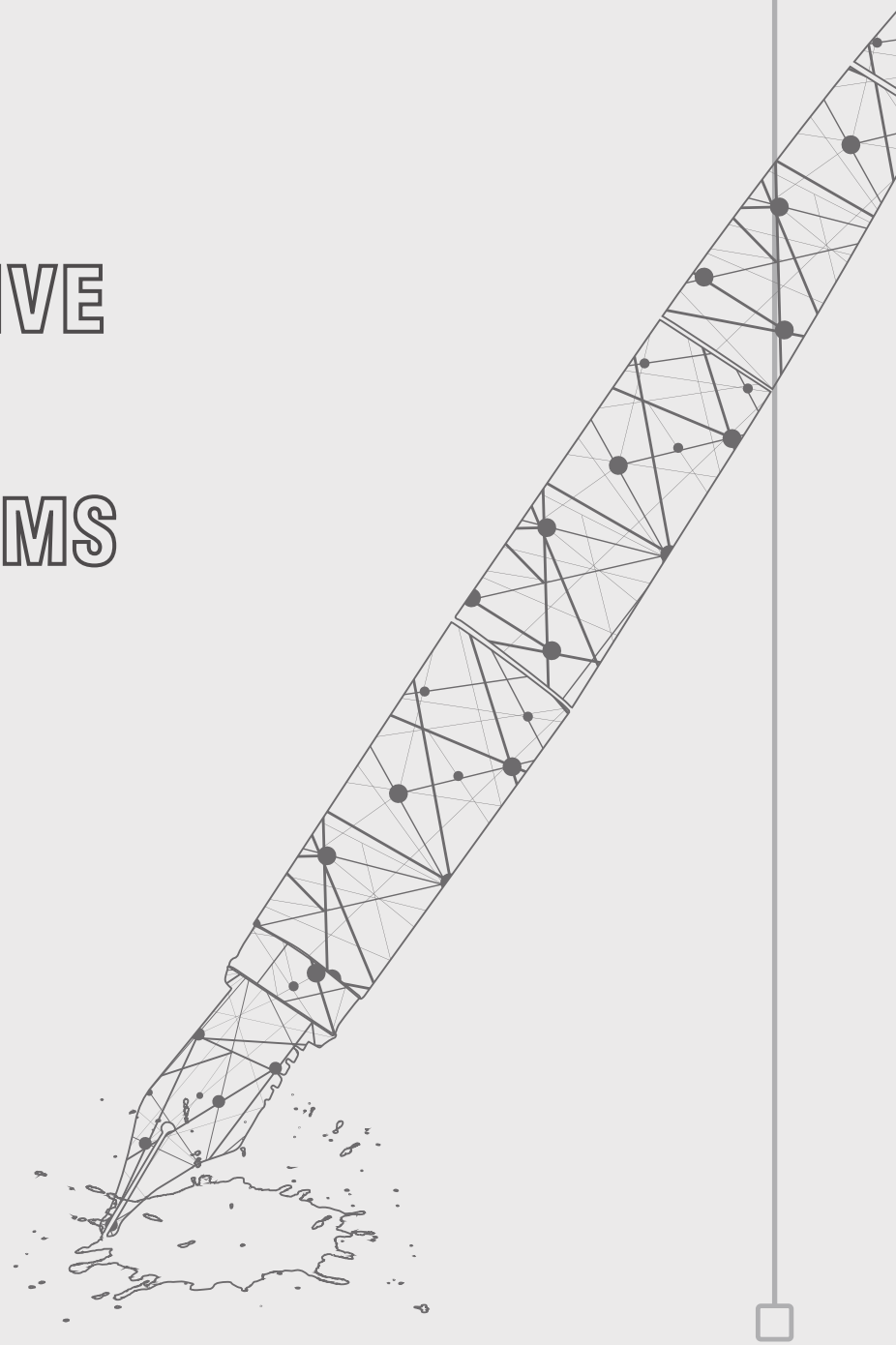
The need for data localisation to achieve this end has, however, come into question in light of new thinking on the exercise of taxation powers in the digital economy.

The Finance Act, however, introduced an amendment to incorporate the aspect of 'significant economic presence.' Section 9, Explanation 2A of the Income Tax Act states that a significant economic presence of a non-resident in India would already constitute a business connection, therefore making the income taxable in India. Hence, the logic behind mandating storage in India to tax the digital transaction is unwarranted, as India has also adopted an 'equalisation levy' since 2016 that ensures the imposition of tax on advertising revenues earned by foreign firms in India through business carried out in India without a permanent establishment in India.[114]

[114] *"Data localisation in India: Questioning the means and ends - NIPFP." 31 Oct. 2018, https://www.nipfp.org.in/media/medialibrary/2018/10/WP_2018_242.pdf. Accessed 15 Nov. 2018.*

CHAPTER 6

ALTERNATIVE POLICY MECHANISMS



6.1 Reforming the MLAT Process

MLATs are strategic agreements entered into between states to exchange evidence for criminal investigations and prosecutions.[115]

An MLAT is an international level agreement between two or more countries to facilitate the exchange of information and persons for the enforcement of laws in the participating countries. MLAT may be bilateral, multilateral or regional. The idea behind entering into an MLAT is to establish cross-border cooperation for the enforcement of laws. An MLAT sets up a formal mechanism for sharing and access to information and data between the participant countries. The MLATs have assumed great importance and significance in recent times where the law enforcement agencies across the world are fighting common concerns of international terror and violence[116]. The Image 4 below shows an example of MLAT process between the United States of America and a country (Country A, for example) seeking a request to access data. The US incorporates administrative and judicial entities to process a request to access data.

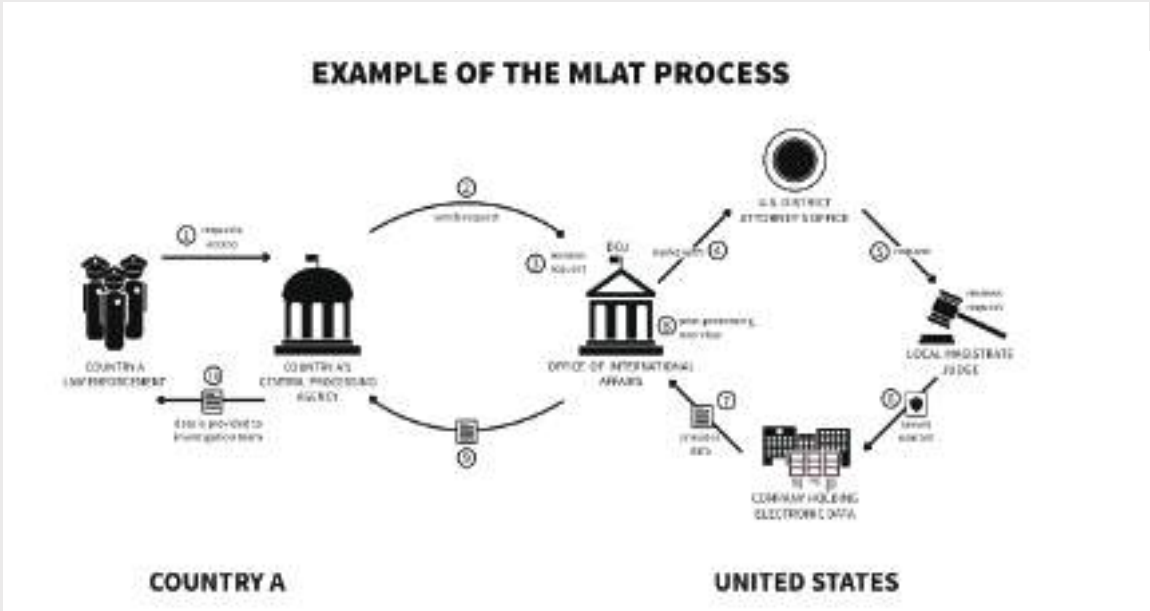


Image 4: Example of MLAT process between the US and the country seeking a request to access data

Generally, an MLAT contemplates a designated agency ("Agency") in each state (country) to handle requests for access and sharing of information and specifies the general procedure to be followed in such cases.[117]

As per the common general procedure specified in the MLATs, the Agency in the requesting State is required to requests information from the Agency Authority in the requested State in the specified format. An

MLAT usually specifies the nature and quality of information that is required to be provided along with the request. The receiving State determines whether there is a legitimate reason to deny the request for information. If not, they process the request. Sometimes the requesting state may seek a witness for a trial. In such a case, the MLAT will generally contain guidelines for transporting the person or in some instances will provide procedures for remote testimony.[118]

While MLATs may be useful for mutual legal assistance in the generic sense, the effectiveness of MLATs in the current times has come under question. The nature of crime and criminals have evolved considerably, and therefore it is essential that aspects relating to information technology, data transfer, etc., are factored into the MLATs. The aspects relating to when data can be shared, with whom, and on what terms, need to be made more transparent and result yielding. The effectiveness of MLAT often comes under scrutiny due to the lengthy and laborious processes involved that have exacerbated the challenges for making it work.[119]

The position of MLATs in India

The Ministry of Law and Justice administers the MLATs in India in the civil and commercial matters, and the Ministry of Home Affairs is the nodal Ministry and the central authority for seeking and providing mutual legal assistance. The Ministry of Home Affairs receives all such requests, examines them and takes appropriate action in criminal matters.[120]

The requests for seeking assistance from a foreign country including the service of all kinds of judicial processes or other documents are directly submitted to the Ministry of Home Affairs in criminal law matters and the Ministry of Law & Justice in civil and commercial matters. The Ministry of External Affairs may be involved in this process when such requests are routed through diplomatic channels by these Ministries.

Section 105 of the CrPC deals with reciprocal arrangements to be made by the Government of India with the governments concerning the service of summons/warrants/judicial processes. India currently has MLATs with 35 countries in the world,[121] including the United Kingdom, the United States of America, the French Republic, United Arab Emirates and the Republic of Singapore.

A common feature in most of these MLATs is that scope of cooperation is quite extensive. However, generally, no timelines and time limits are mentioned for responses and fulfillment of requests.

The Indian law enforcement agencies rely on the MLATs to seek information and cooperation from Agencies in other countries with whom India has an MLAT. In order to investigate a crime, the law enforcement agencies may need access to the data that is stored on the servers outside India under the ownership and control of entities or persons outside India in other jurisdictions.[122]

Challenges

1. Application Process Insufficient:

From the bilateral side, the primary concern that has been raised is the suboptimal application process from the Indian law enforcement side to other nations for law enforcement requirements. India has an active MLAT process with the US government, since US companies constitute of the majority of processing of Indian data.

When responding to requests for user data, companies verify whether the requisite details, such as authorised government id, mail drafted on letterhead, name, rank and identification of officer and case number - have been provided

in the requests.[123]

Companies reject such requests unless the due procedure is followed.

2. Structural Challenges

At the moment, India does not have a dedicated cell or a body within the Ministry of Home Affairs that looks after the process of MLAT. While the US State Department has three full-time staff that cater to Indian law enforcement agencies' data sharing requests, the Indian government is yet to institutionalise this process more deeply into its system. Due to lack of a structural process, the applications submitted by the Indian side often fails to live up to the mark, making it difficult for US State Department to execute the process.

Review and Reforms

Given the importance of the purpose and the objective that MLATs serve, it is imperative that the MLATs be seen as an effective means of facilitating sharing and access to data and information between the countries. There are certain aspects on which the MLATs may be refreshed, reformed and tuned to meet the requirements in the present time. Some of such aspects are listed hereinafter:

(i) Certainty and Consistency

In order for MLATs to be considered as useful and relevant in the context, it is critical to grant certainty to practices and procedures and minimize discretion. Certain specific situations may be spelt out wherein the Agencies have to act in a time-bound manner as long as the prescribed procedure for requesting information and access has been followed. The conditionality and procedural for the sharing of personal data by the host country to the Agency of a foreign country needs to be mentioned without any ambiguities. The requirements, procedure and timelines for emergencies may be separately identified and prescribed. Gradually, the countries of the world may move towards a harmonised system of storage and access to specific selective critical data.

The aspects relating to interception or access to data on the cloud may be specifically addressed in the existing MLATs especially in the MLATs with the countries which are leaders in the sector.

(ii) Resources and Implementation

The country parties to the MLATs should ensure sufficient infrastructure and resources to honour the obligations under the respective MLATs. It would be futile to have a comprehensive MLAT with a country which is unable to deploy sufficient resources to meet its obligations under the said treaty. While allocating or designating resources, any form of multiplicity of authorities needs to be avoided. A single point of contact system is certainly preferable. The persons at the Agency involved in the MLAT procedures should be sufficiently trained and equipped to understand and appreciate legal aspects and issues. In order to bring transparency and swiftness to working of MLATs, the processing and tracking of MLATs requests and all related procedures and proceeding may be digitised.

(iii) Minimizing Conflict between Domestic Laws and Treaty Obligations

In order to create an effective MLAT regime, it is critical to minimise situations of conflict between the treaty obligations and domestic laws. In specific cases, recognition of foreign awards is promoted to avoid duplication of legal proceedings. The aspects of accountability and judicial oversight may be incorporated in the domestic legal regime oversight along with the right to the legal

remedy so that contentious issues may be resolved conclusively.

(iv) Enhanced Capacity Building

Indian law enforcement agencies must build capacity within state and central agencies, institutionalizing inter-agency cooperation. O cers should be trained to be clear and specific in drafting requests. The Ministry of Home Affairs (MHA) should also build capacity and expertise to receive and review requests, establishing a dedicated team of legal officers trained in international criminal law and law enforcement agents on deputation. The MLAT process can be significantly transformed if it is digitized, requests for supplementary information are streamlined and internal time limits are introduced.

It may be essential to review the domestic legal regime and the treaty and amend if required, the same to avoid any potential conflict concerning governing laws and jurisdiction of courts.[124]

Besides, MLATs should be sufficiently detailed to resolve differences in the interpretation of laws and electronic systems should also be looked at with its implementation.

[115]"*Treaties and Agreements - US Department of State.*" *7 Mar. 2012, https://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm. Accessed 15 Nov. 2018.*
[116]"*FAQs - MLAT.*" *https://www.mlat.info/faq. Accessed 15 Nov. 2018.*
[117]"*Ex. Rept. 107-15 - MUTUAL LEGAL ASSISTANCE TREATIES WITH ....*" *https://www.congress.gov/congressional-report/107th-congress/executive-report/15. Accessed 15 Nov. 2018.*
[118]"*mutual legal assistance - US Department of State.*" *https://www.state.gov/documents/organization/111634.pdf. Accessed 15 Nov. 2018.*
[119]"*Mutual Legal Assistance Treaties (MLATs) - Carnegie Mellon ....*" *14 May. 2015, https://www.heinz.cmu.edu/~acquisti/SHB2015/Swire.docx. Accessed 15 Nov. 2018.*
[120]"*mutual legal assistance requests - The Ministry of External Affairs.*" *http://mea.gov.in/Images/pdf1/MUTUAL_LEGAL_ASSISTANCE_REQUESTS.pdf. Accessed 15 Nov. 2018.*
[121]*Central Bureau of Investigation – India, MLATs, http://cbi.nic.in/interpol/mlats.php*
[122]"*MLATs - Observer Research Foundation.*" *8 Aug. 2017, https://www.orfonline.org/wp-content/uploads/2017/08/MLAT-Book.pdf. Accessed 15 Nov. 2018.*
[123]"*Hitting Refresh - Observer Research Foundation.*" *8 Aug. 2017, https://www.orfonline.org/wp-content/uploads/2017/08/ORF_SpecialReport_39_DataSharing.pdf. Accessed 15 Nov. 2018.*
[124]*Primary Input*

6.2 Multilateral Cooperation on Data Sharing and Information Access

Regulatory frameworks for data privacy are critical to facilitate cross-border data flows in Asia and around the world. Over the past decade, international data flows have increased global GDP by 10.1 per cent. Data flows accounted for US$2.8 trillion of global GDP in 2014, a larger share than the global trade in goods.[125]

Achieving greater clarity on international data transfer procedures and alignment with international standards and laws could provide a great fillip for the data processing industry in India. Governments in Asia have worked hard to develop and implement data privacy frameworks that can adequately protect the data of their citizens, while also allowing data to own across-borders in ways that support trade and innovation. These frameworks encourage convergence across the region, which enables data to ow while maintaining a similar level of protection.

Presently, there is no comprehensive provision exists in Indian law that regulates the transfer of personal data outside of India. However, the authors feel that for India to successfully leverage its position as a global leader in the digital space, it is imperative to chart out a roadmap for cross-border data flow, to and fro India.

A pivotal alternative to data localization concerning access to data could be in the form of bilateral or multilateral data sharing agreements with member states.

It is indeed entirely possible to develop and successfully maintain a system of voluntary cross-border transfer of personal information when law-enforcement requires it for justifiable criminal investigations. Several countries have data sharing and data transfer agreements in place to help them gain faster access to data in question for criminal cases. The United States and the UK have a Cyber-Cooperation Agreement in place since 2016 for justified review of an individual's data for criminal investigations. The CLOUD Act in the United States allows US law-enforcement agencies, with the right paperwork and legal justification, access to an individual's data from US-based agencies regardless of where it is stored around the world. These new treaties addressed the prior issue of relying on MLATs (Mutual Legal Agreement Treaty) for an exchange of information – which was usually a long, and heavily bureaucratic process.[126]

India can enter similar agreements with countries to ensure criminals are appropriately brought to justice while protecting an individual’s right to privacy and promoting GDP growth.

India could sign a data sharing agreement under the Cloud Act, 2018 after fulfilling certain eligibility conditions given under the Act which include domestic privacy protection laws, substantive and procedural laws on cybercrime and electronic evidence, accountability and transparency mechanisms.

6.2.1 Interoperability with APEC

India should focus at harmonising its domestic data protection standards with the APEC and ASEAN nations with an eye on interoperability with the APEC Cross-Border Privacy Rules (CBPR) system developed by the Asia-Pacific Economic Cooperation (APEC) forum. The CBPR is a fast-growing cross-border transfer

mechanism for the entire APEC region, which comprises 21 member economy and more than half of the world population and economy.[127]

CBPR is an enforceable code of conduct that provides for interoperability of cross-border data transfers that have been reviewed and certified by an approved third-party certification organization (Accountability Agent).[128]

Enforcement of the CBPR is provided by APEC data protection and privacy authorities that have joined the APEC Cross-border Privacy Enforcement Arrangement (CPEA). The advantage is that it allows transfers not only within a global corporate group (or within a group of enterprises engaged in "joint economic activity") (such as under the BCR), but also between unaffiliated companies and to companies that are not CBPR-certified anywhere in the world.

Non-APEC countries that adopt similar mechanisms could make their cross-border rules mechanisms interoperable with the CBPR (and other similar schemes) if and so long as there is substantial overlap in the data protection requirements within each system.[129] This will have the effect of creating a global certification mechanism requiring only one approval process. The EU and APEC have taken initial steps to explore and develop interoperability between EU transfer mechanisms (e.g., BCR and future GDPR certifications) and the APEC CBPR.[130] India should look to include a transfer mechanism modelled on the CBPR in its data protection law to enable such future interoperability between the APEC region and India.

[125] *"Regional Privacy Frameworks and Cross-Border Data Flows - GSMA." https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Exec-Summary_Sept-2018.pdf. Accessed 15 Nov. 2018.*

[126] *"Cross-Border Data Flows: Where Are the Barriers, and What Do They ...." 1 May. 2017, https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost. Accessed 15 Nov. 2018.*

[127] *"Singapore Joins APEC Data Privacy System - Asia-Pacific Economic ...." 7 Mar. 2018, https://www.apec.org/-Press/News-Releases/2018/0307_CBPR. Accessed 15 Nov. 2018.*

[128] *"The APEC Cross-Border Privacy Rules—Now That We have Built It, Will ...." https://iapp.org/news/a/the-apec-cross-border-privacy-rules-now-that-weve-built-it-will-they-come/. Accessed 2 Nov. 2018.*

[129] *"As Asia-Pacific rises and integrates, so too could the APEC Cross ...." 30 Oct. 2018, https://iapp.org/news/a/as-asia-pacific-rises-and-integrates-so-too-could-the-apec-cross-border-privacy-rules/. Accessed 15 Nov. 2018.*

[130] *"International data-sharing norms: from the OECD to the General Data ...." 1 Aug. 2018, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6132662/. Accessed 2 Nov. 2018.*

6.3 Incentivising Data Storage Through progressive policy-making

The government should consider incentivising local data storage in India as opposed to enforcing it with a will. There are gaps in the physical infrastructure, legal security of data, enormous energy demand that will put a strain on India's energy situation, physical safety.

In this section, the author(s) have identified specific conditions that the government must try to fulfill before mandating localisation in India.

6.3.1 Tax Incentives

Central and state government in India could explore the option of reducing tax rates for companies that operate data centers in India, thus making it lucrative for organisations to invest in India's data center industry. For example, in the US, there is explicit competition between states to offer better incentives for data centers. While state governments can do little to change fundamentals like the climate, the available energy and the price of real estate, they can do a lot with taxes.

Tax measures that boost renewable energy and efficiency are a recurring theme. If done right, this could be seen as a win-win situation, encouraging business in, and persuading it to operate more cleanly.

In Arizona, Apple benefited from sizeable tax incentives when it started investing $2 billion in its new command center. Measures from 2013 meant it would be exempt from sales and use tax on data center-related equipment purchases for ten years (since extended to 20 years).[131]

6.3.2 Robust Infrastructure

Land Availability

The growing data center market in India will require real estate players to build out capacity to meet the needs. India requires more straightforward land acquisition policies that can enable organisations to set up and operate data centers in India. Policymakers could look at introducing specific incentives, such as allocating large tracts of land in different parts of the country for data centers and subsequently providing a faster and simpler process for acquiring such tracts of land.

Power Access

Power access, similar to land acquisition, is another challenge that needs to be overcome before data centers could evolve in India. Ensuring 24/7 power supply 365 days a year with backup options is a significant challenge that must be overcome.

6.3.3 Legal Security of Data

Indian Government must identify guidelines that protect and secure the legal status of data residing and stored in India. Presently, India does not have a due process of law through which data stored in India should be protected under law. Such provisions must be enacted by law in the Parliament and enforced strictly by the state. Unless the state guarantees that data is secure in India through a legal process, only then can we expect greater trust and confidence amongst the global organisations that control and process data to provide solutions.

6.3.4 Modernisation of Existing Infrastructure

Existing data centers must become more agile while controlling costs and keeping up with the trends to stay competitive. Data center modernization and consolidation involves customizing data center strategies according to business goals, regulatory requirements, and skills availability. Those businesses that assess the trends save more than 10% of their annual operational costs.

[131] *"Do data center tax breaks help? - DCD." 27 May. 2015, https://www.datacenterdynamics.com/opinions/do-data-center-tax-breaks-help/. Accessed 2 Nov. 2018.*

6.4 Generate in India - Process in India

The growth of smartphone penetration in India has directly resulted in a massive increase in the amount of data being generated. This number is only set to grow further as high-speed internet services are becoming more accessible and easily affordable in both urban and rural areas. Globalisation, economic growth, and the availability of easy-to-use, low-cost smartphones are also playing a significant role in driving greater data generation in the country.[132]

Presently, Indian customers are catered mostly by international service and solution providers across the range of services available on the internet. This includes social media, payments system, e-commerce platform, search engines for research purpose, cloud computing and storage as well as storage and transfer of data. From a data consumer, India needs to emerge as a data processor oriented economy. Under the Hon'ble Prime Minister Modi's ambitious Digital India programme, enabling India into a digital ecosystem powerhouse is a crucial objective. To achieve this objective, data localisation is not the answer, but self-reliance through developing indigenous services is the way to move forward.

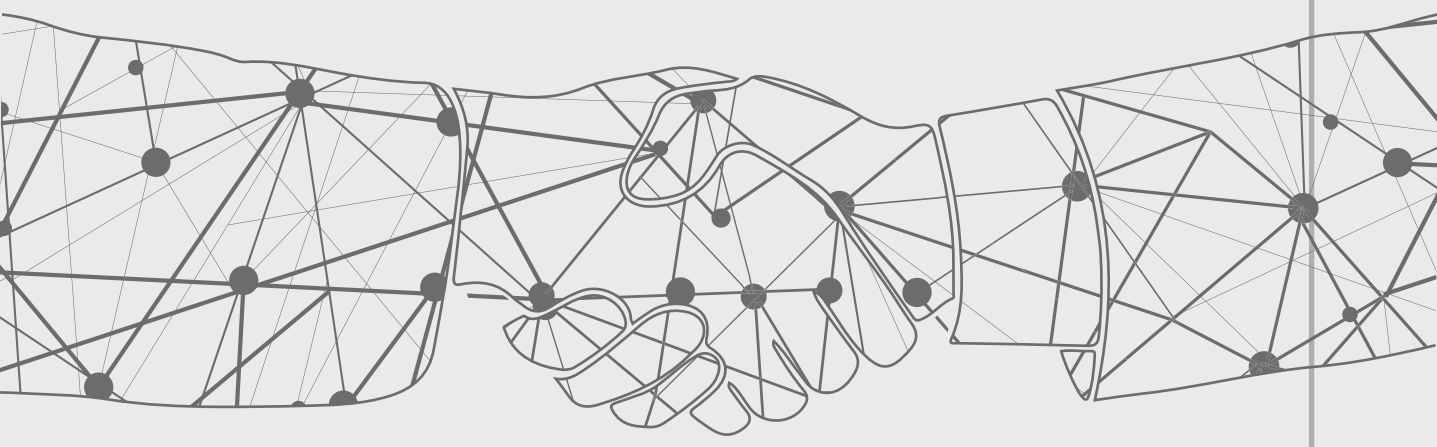
We are indeed witnessing a rise of Indian made services providers, including social media apps, that offer various range of services to users. Apps such as Hike and Sharechat have the potential to give global giants a run for their money.

Indian government should focus on encouraging the development of local talent to help create a robust digital economy infrastructure, whose is foundation is laid by Indian made apps and services. While at the same time, keeping the doors open for offering players to deliver services in India and allowing free-flow cross-border data exchange between multiple jurisdictions.
Subsequently, by reforming domestic policies to allow competition to prosper, Indian service providers may also benefit from reciprocal stance by foreign governments, which can allow them to enter new markets.

[132] *"5 factors driving the growth of data analytics in India - YourStory." 16 Dec. 2016, https://yourstory.com/2016/12/growth-data-analytics-india/. Accessed 2 Nov. 2018.*

CHAPTER 7

GREATER INTERNATIONAL COOPERATION



7.1 Introduction

For India to leverage its position as a global leader in trade and technology, one area where the greater emphasis needs to be demonstrated is forming international alliances towards data sharing cooperation.

This chapter is an extension of the points raised by the authors in Section 6.3. The premise of our arguments is based on driving international cooperation based on the domestic adequacy and a strong privacy regime. Data localization does not work in isolation. The impact is global, and the stakeholders involved are also multifaceted. Maritime law and international trade originated from universally recognised principles across-borders and were later given the force of law by way of UN charters and international treaties.

Governments in Asia are working to develop and implement data privacy frameworks that can adequately protect the data of their citizens, while also allowing data to allow across-borders in ways that support trade and innovation. These frameworks encourage convergence across the region, which enables data to ow while maintaining a similar level of protection.

7.2: Why Cross-border Data Flow Matters in Asia?

Across Asia, data privacy discussions are gaining traction, at both domestic as well as bilateral and multilateral level. This primarily includes ASEAN and APEC countries. The advantage of driving a privacy regime at a global level in Asia will help member countries' approach to data protection, reduce barriers to investments in the short and medium run along with a more specific compliance environment for businesses that wish to operate in that country.[133]

Asia is transitioning to be the growth engine of the world in the 21st century.

Leveraging existing international mechanisms, such as the APEC's Cross-Border Privacy Rules, standard contractual clauses recognized by the European Commission,34 and binding corporate rules (recognized under the EU's GDPR and also by Israel), rather than creating national versions of these same mechanisms.

[133] *"GSMA: Free Flow of Data Across Borders Essential for Asia's Digital ...." 5 Sep. 2018, https://www.gsma.com/news-room/press-release/gsma-free-flow-of-data-across-borders-essential-for-asias-digital-economies/. Accessed 15 Nov. 2018.*

7.3 Towards a Multilateral Privacy Framework

For India to successfully seek access to data, the author(s) herewith recommend developing a multilateral data-sharing framework based on the principles of adequacy and reciprocity.

Globally, countries are moving towards regional and multilateral data sharing and privacy frameworks that support cross-border data flow between those jurisdictions that deploy a high-standard of privacy regime .

The OECD encourages countries to restrain from restricting data flows where there are sufficient safeguards and if the other country also observes similar guidelines. Similarly, the APEC provides that governments should ensure that there are no unreasonable impediments to cross-border data transfers while protecting the privacy and security of personal information. The ASEAN Framework objective is to *"strengthen the protection of personal data in ASEAN and to facilitate cooperation among the participants, intending to contributing to the promotion and growth of regional and global trade and the flow of information"*[134] though it does not explicitly address restrictions on data flow.

However, the GDPR and to a lesser extent Convention 108 are more restrictive in the transfer of personal data of EU citizens to third countries or international organisations unless they meet a set of conditions, in order to ensure that the level of protection of individuals provided by the GDPR is not undermined.[135]

The conditions – which are legally enforceable – include the designation by the European Commission that a country meets an "adequate" level of personal data protection, or where standard contractual clauses or Binding Corporate Rules (BCRs) exist. It should be recognised, however, that the EU approach also prohibits restrictions on data flows between Member States/Parties.[136]

More significantly, the White Paper released by the Justice Srikrishna Committee deals with the issue of cross-border data protection and asks numerous questions for consultation related to it. The paper recognises that providing strong rules to protect cross-border data flows is vital for small and medium-sized enterprises or "SMEs," consumers and multinational businesses. The paper opines that the adequacy test is particularly beneficial and the proposed data protection authority should be able to determine it to ensure a smooth two-way flow of information, critical to a digital economy. The paper seeks views and public consultation on issues such as specific provisions facilitating the cross-border transfer of data and cross-border flow of sensitive personal data.

The primary issue in formulating a multilateral privacy framework for data sharing at the regional, continental or global level remains the same, i.e., alignment of a nation's right to territorial sovereignty with global cooperation.

A multilateral privacy framework assumes great significance on account of the following key attributes of cloud data storage:

(i) Multiplicity - whereas physical information generally exists in one place at one time, data can be stored in multiple places at one time. Consequently, accessing the contents of a single, apparently unitary account may require retrieval of data stored on the territory of multiple sovereigns.

(ii) Attribution and Traceability - there need not be any correspondence between the physical storage location of a data principle data and data principles physical location.

(iii) Automation – since cloud data is partitioned,

stored, and moved automatically by algorithms, in several situations, it may be difficult for one to confirm with certainty the physical location of the data.

(iv) Anonymity - the identity, nationality, and residency of a data principle may not be known to the data processor or the data fiduciary.

Data in today's time and age is a commodity and consequently needs to be regulated not only at a bilateral level but at a multilateral level because the flow of data is seamless and without borders. Given the nature of technology and resultant blurring of territorial boundaries in case of data traffic and storage, it is essential for law enforcement agencies to have means and mechanisms for accessing the data and information beyond their territorial jurisdiction.

The current generation of Mutual Legal Assistance Treaties ("MLATs"), which were designed to facilitate the transfer of tangible evidence across borders, are functionally obsolete. The need for the hour is to have multilateral arrangements specifically for data sharing in light of the nature and attributes of digital data mentioned above and privacy and security issues.

Any multilateral data sharing framework must be based upon the following fundamental principles:

(i) Certainty and conclusiveness in the process for requesting and executing the data access and sharing requests.

(ii) International security, terrorism, and money laundering should be universally accepted and adopted grounds for data access.

(iii) Surveillance, other than preventive surveillance should be prohibited.

(iv) Reasons of refusal to grant access may be specified as a 'negative list.

(v) Manner and procedure for functional implementation may be specified.

Several organisations and entities have done quite a directional work in this field and have come up with interesting findings and propositions. Some of such noteworthy projects are as follows:

(i) Findings of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.[137]

(ii) The MAPPING (Managing Alternatives for Privacy, Property and Internet Governance) Project.[138]

(iii) The Draft Legal Instrument on Government-Led Surveillance ("LI")[139] - The LI suggests the creation of an International Data Access Warrant ("IDAW") that governments can use to obtain private data for investigative purposes. The current LI further suggests the creation of an International Data Access Authority composed of retired judges from the contracting states who would evaluate IDAW applications against international human rights norms before authorizing them.

[134] "*framework on personal data protection - asean.*" *https://bit.ly/2Dq8Wdt Accessed 15 Nov. 2018.*
[135] "*Top 10 operational impacts of the GDPR: Part 4 - Cross-border data ....*" *https://bit.ly/2DokVbq Accessed 15 Nov. 2018.*
[136] "*(PDF) Access to Electronic Data by Third-Country Law Enforcement ....*" *https://bit.ly/2PyoP8X Accessed 2 Nov. 2018.*
[137] "*Group of Governmental Experts on Developments in the Field of ....*" *9 Apr. 2017, https://bit.ly/2zcA90a. Accessed 15 Nov. 2018.*
[138] "*Managing Alternatives for Privacy, Property and INternet Governance ....*" *https://cordis.europa.eu/project/rcn/111214_en.html. Accessed 15 Nov. 2018.*
[139] "*the drafting of a Legal Instrument on Government-led Surveillance and ....*" *10 Jan. 2018, http://www.ohchr.org/Documents/Issues/Privacy/DraftLegalInstrumentGovernmentLed.pdf. Accessed 15 Nov. 2018.*

7.4 How Can India Lead a Regime?

The law which will govern data, its usage in India is still in the form of a bill. For it to be at the forefront of governance of data, India will have to enact a law which is robust in tackling security and flow of data, and at the same time can balance the rights of its citizens giving them a say in how their data will be used. The Bill, once enacted, can thus be the model or guiding law for regional and other countries to create a data regulation regime. Further, India will have to invest heavily in capacity building regarding raising workforce who understand the nuances of this sensitive matter and also build institutions which can handle this domain, which is still evolving and is likely to face much push and pulls.

The manner in which India took the initiative and decisive steps to amend the double taxation avoidance agreement with countries like Mauritius and Switzerland to ensure adequate disclosure and exchange of specified financial information between the countries can be an excellent guiding principle and foundation for creating robust multilateral data sharing regime.

7.5 Enabling Global Data Sharing Agreement

Cross-Border data flows are a two-way street, and for countries to share data with each smoothly, foreign jurisdictions should also come forward and play a part in helping India mainstream its global data sharing process.

Data sharing agreements are bilateral or multilateral engagements between countries that provide mechanisms for governments to gain access to data held in another jurisdiction. This is especially important for Indian law enforcement requirements. A critical fundamental aspect, however, is that countries entering into such engagements should have similar standards of privacy, to avoid situations in which fulllment of these requests by one government would undermine its domestic privacy, cyber-security, and data protection standards.

India has been an observer to the Asia-Pacific Economic Cooperation ("APEC") Cross-border Privacy Enforcement Arrangement since November 2011. Since the inception, India has expressed interest in joining APEC. In the recent past, there have been increasing reports of the conditions being favourable for India to be a part of APEC, in which case there may be a possibility of it joining the Cross-Border Privacy Rules System.[140]

India is also a member of the Association of Southeast Asian Nations ("ASEAN") Plus Six group. So far, there has been no clear avowal of the ASEAN Framework on Personal Data Protection by India. For now, India has not been recognised by the European Union ("EU") as offering an adequate level of protection in the application of Article 25(6) of Directive 95/46/EC.[141]

India has been seeking this status for some years through trade agreements with the EU, as the lack of such a status leads to higher operating costs for Indian companies handling EU data and impacts their ability to compete for business from European data controllers.[142]

Indeed, 30% of India's US$100b information technology ("IT") and business process outsourcing industry comes from customers based in the European market. In 2012, the Data Security Council of India estimated that the outsourcing business can further grow by US$50b per annum if India is recognised as a "data secure" destination by the EU. This is even more important as India, which has a strong track record of performing low-end data processing in the EU, desires to move up the value chain into more sophisticated outsourced work in sectors such as healthcare, clinical research, and engineering design.[143]

In this regard, the proposed U.S.-UK data-sharing agreement gives U.S. law enforcement access to data held in the United Kingdom concerning U.S. citizens, and vice versa. The agreement would allow U.K. companies to hand over data on U.S. citizens to U.S. law enforcement officials, upon presentation by the U.S. officials of a domestic (U.S.) warrant.

How can India enter into such an agreement with the US? The process is as follows:

1. Qualify Under CLOUD Act - India should focus at qualifying under the US CLOUD Act that provides for easier access to data for law enforcement purposes as it bypasses the government machinery and allows executive agreements with the U.S. that would allow them to submit requests for electronic data, both stored and intercepted live, directly to U.S. companies.[144]

2523 of the Cloud Act[145] sets out a lengthy list of requirements for the content of executive agreements (ex: confidentiality of the data, requirements for the foreign government's request, rights and obligations of each party, etc.).

• The foreign government's law must afford "robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement."[146]

• The section goes on to list these protections such as "adequate substantive and procedural laws on cybercrime and electronic evidence, as demonstrated by being a party to the **Convention on Cybercrime, done at Budapest November 23, 2001** (…) international human rights obligations and commitments or demonstrates respect for international universal human rights (…) sufficient mechanisms to provide accountability and appropriate transparency regarding the collection and use of electronic data by the foreign government"

• The foreign government has adopted "appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons subject to the agreement"; and

• Orders subject to the executive agreement must comply with rigorous conditions such as "not intentionally target a United States person or a person located in the United States", be "for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism" and "shall be subject to review or oversight by a court, judge, magistrate, or other independent authority".[147]

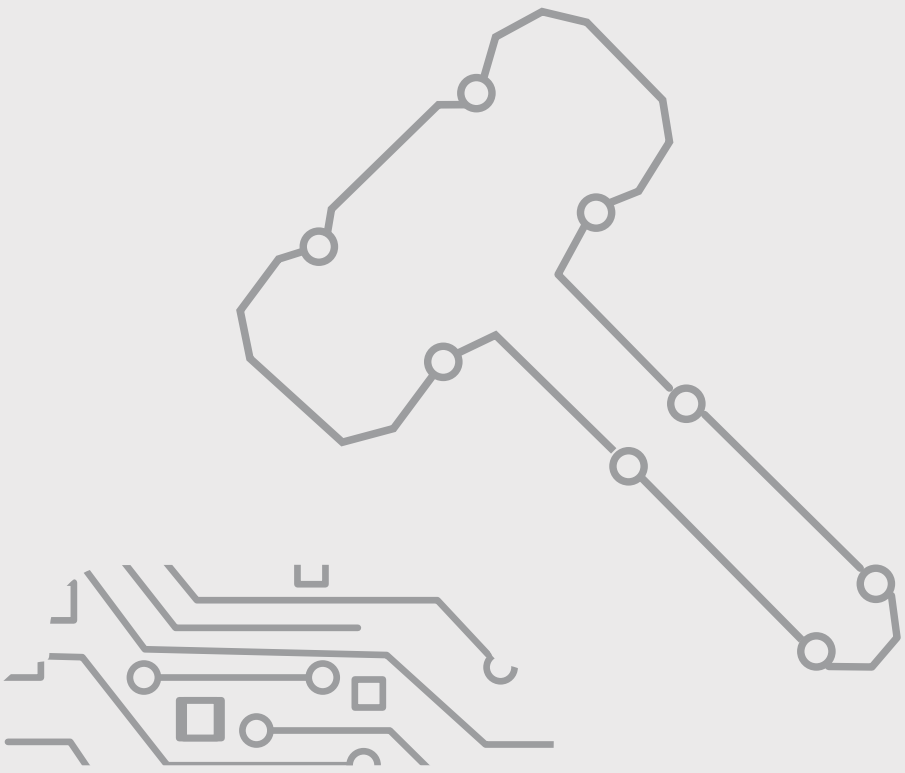
2. Once the above conditions are fulfilled, the proposed country can then enter into an executive agreement with the USA under the CLOUD Act to seek access to data. For India, this means that first, the government will have to analyse post passing of the data protection bill whether it meets the criteria or not. Once it does, then it should activate the process for enabling an executive agreement under the CLOUD Act.

The CLOUD Act responds to calls for modernization by authorizing the executive branch to conclude a new form of the international agreement through which select foreign governments can seek data directly from U.S. technology companies without individualized review by the U.S. government. Agreements authorized by the CLOUD Act would remove legal restrictions on certain foreign nations' ability to seek data directly from U.S. providers in cases involving "serious crimes" when not targeting U.S. persons, provided the Executive has determined that the foreign nation's laws adequately protect privacy and civil liberties, among other requirements.

[140] *"Glossary - Asia-Pacific Economic Cooperation." https://www.apec.org/Glossary. Accessed 2 Nov. 2018.*
[141] *"Promoting stability in ASEAN's cyberspace | Clingendael spectator." 23 Aug. 2018, https://spectator.clingendael.org/en/publication/promoting-stability-aseans-cyberspace. Accessed 2 Nov. 2018.*
[142] *"EU-India relations, factsheet - European External Action Service." https://bit.ly/2DHTj1L Accessed 2 Nov. 2018.*
[143] *"Renewable energy country attractiveness index (RECAI) 43 - EY." https://go.ey.com/2DKxdfp Accessed 2 Nov. 2018.*
[144] *"Cross-Border Data Sharing Under the CLOUD Act - Federation Of ...." 23 Apr. 2018, https://fas.org/sgp/crs/misc/R45173.pdf. Accessed 2 Nov. 2018.*
[145] *"Text - H.R.4943 - 115th Congress (2017-2018): CLOUD Act ...." 6 Feb. 2018, https://www.congress.gov/bill/115th-congress/house-bill/4943/text. Accessed 2 Nov. 2018.*
[146] *"18 U.S. Code § 2523 - Executive agreements on access to data by ...." https://www.law.cornell.edu/uscode/text/18/2523. Accessed 15 Nov. 2018.*
[147] *"What are executive agreements under the Cloud Act ? - Mathias Avocats." 25 Jun. 2018, https://www.avocats-mathias.com/actualites/executive-agreements-cloud-act. Accessed 2 Nov. 2018.*

CHAPTER 8

BEST PRACTICES FOR DATA STORAGE IN INDIA



8.1 Due Process of Law for Access in India

Another knotty issue in data processing is due process to access data. To protect privacy, as guaranteed by the Supreme Court in the Puttaswamy judgement, due process of law to seek access to data is fundamental. The data in question can be sensitive and a process has to be put in place to ensure that the data is not readily made available to unauthorised persons and also to ensure that such limitations to access data should not come in the way of dispensation of justice or rendering of any critical service such as compliance of judicial order. Due process may, in turn, lead to greater control of citizen is over their data by data fiduciaries.

As per the current judicial trend and jurisprudence, as enshrined in the various judgements passed by the courts in India, in order to be valid and enforceable, any hindrance or restriction on an individual's right to privacy should satisfy the following essential conditions:

(i) The restriction should be based on the principle of minimum intrusion.

(ii) The restriction must be authorised and backed by law;

(iii) The restriction must be demonstrably necessary and justified;

(iv) The restriction must not be excessive and should be directly linked and proportionate to cause;

(v) The restriction must be concerning and towards a legitimate state interest.

The Bill contains several enabling provisions allowing processing (as defined under the bill to include collection, storage, disclosure, etc.,) of personal data in the interest of 'Security of State.' It is interesting to note that the Bill does not contain any provision citing situations for exemption from processing of personal data for security of state, but apparently provides that processing of personal data in the interests of the security of the State shall not be permitted unless it is authorised pursuant to a law, and is in accordance with the procedure established by such law, made by Parliament and is necessary for, and proportionate to, such interests being achieved.

The Bill seems to have effectively deferred a contentious issue for a more extensive legislative process. The Bill, it is felt, ought to have laid out comprehensive provisions relating to data protection and could have provided for certain aspects to having been taken care of through the process of delegated legislation. In view of the provisions of Section 42 in the Bill, it would be virtually impossible (and illegal) for surveillance entities to carry out their activities even though extremely critical in the interest of 'Security of State.' A judicial/regulatory mechanism could have been laid out detailing the following:

(i) An inclusive definition of the phrase 'Security of the State.'

(ii) The entities/bodies which are authorised to process personal data. This list could be an inclusive list with the flexibility of updating the list.

(iii) An inclusive list of situations demanding processing of personal data.

(iv) A safety-net regulatory mechanism to approve processing of personal data (ring-fenced from political or economic influence).

(v) An oversight mechanism.

The courts in India have clearly recognised the prevention, detection, investigations, and prosecution of contraventions of law as an

essential function of the State. It is the duty of the State to ensure public order, safety and security for all persons. There are various laws in India on various subject matters that vest various authorities and law enforcement agencies with the power of to 'process' data for various reasons viz., prevention, detection, investigations, and prosecution of contraventions of law.

Depending upon the nature of contravention of law, there are relevant laws to deal with such contravention. For example, the Code of Criminal Procedure, 1973 ("CrPC") is the general law that describes and details the manner and procedure for investigation and collection of evidence by law enforcement agencies concerning the contravention or suspected contravention of the law. Similarly, there are certain specific laws relating to specific types of offences relating to financial, commercial and tax-related offences (viz., the Income Tax Act, 1963, the Securities and Exchange Board of India Act, 1993, the Prevention of Money Laundering Act, 2002, The Foreign Exchange Management Act, 1999). Each of these specific laws prescribes and authorise the manner of investigation and collection of information and evidence.

Section 43 of the Bill deals with exemptions relating to processing of personal data for prevention, detection, investigation, and prosecution of any offence or any other contravention of law and provides that no such processing shall be permitted unless it is authorised by a law made by Parliament and State Legislature and is necessary for, and proportionate to, such interests being achieved.

From a reading of Section 43 of the Bill, it appears that a balance between the right to privacy and requirement of data processing has been proposed. However, the additional test of proportionality, that has been included may lead to ambiguities and difficulties in implementation and enforcement. It is felt that as long as the due process as laid down in the relevant statute is followed, the test of proportionality may lose significance.

8.2 Legal Security of Data Stored in India

Security of data stored in India can be ensured by following a multi-aspect approach. The law for ensuring security for the data stored in India should address the issues from the following perspectives:

(i) Technical Measures -

Prescribing standards & specifications that need to be complied by the data processors and data fiduciaries. There must be enabling provisions to prescribe the standards and specifications as they evolve.[148]

(ii) Physical Measures -

Prescribing the physical conditions viz., location, situation, construction, layout, etc., of the centers where the data is to be processed.

(iii) Access Control -

Regulating the process & authority for access to and handling of the data being processed.

(iv) Disaster Management & Recovery -

Prescribing the specifications for recovering and damage control in the event of a breach or disaster situation.

Section 31[149] Of the Personal Data Protection Bill, 2018 deals with provisions relating to security safeguards to be followed by data processors and data fiduciaries. However, the Bill does not provide any guidance on the standards or specifications. Putting the onus of 'appropriateness' on the data processors and data fiduciaries may lead to issues in implementation and enforceability. The sensitivity and seriousness of the matter require that specific identified (and evolving) security standards be prescribed in order to bring uniformity in implementation.

Concerning implementing of data protection laws, the following principles laid down by the Organisation for Economic Cooperation and Development ("OECD") may be taken into consideration:

(i) Collection Limitation Principle -

There should be limits to the collection of personal data, and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

(ii) Data Quality Principle -

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

(iii) Purpose Specification Principle -

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

(iv) Use Limitation Principle -

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified explicitly except: with the consent of the data subject; or by the authority of law.

(v) Security Safeguards Principle -

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

(vi) Openness Principle -

There should be a general policy of openness about developments, practices, and policies for personal data. Means should be readily available to establish the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

[148] *"Articles & Publications AUGUST 2018 - Induslaw." 3 Aug. 2018, https://induslaw.com/app/webroot/publications/pdf/alerts-2018/Personal_Data_Protection_Bill_2018.pdf. Accessed 15 Nov. 2018.*

[149] *Security Safeguards.—*

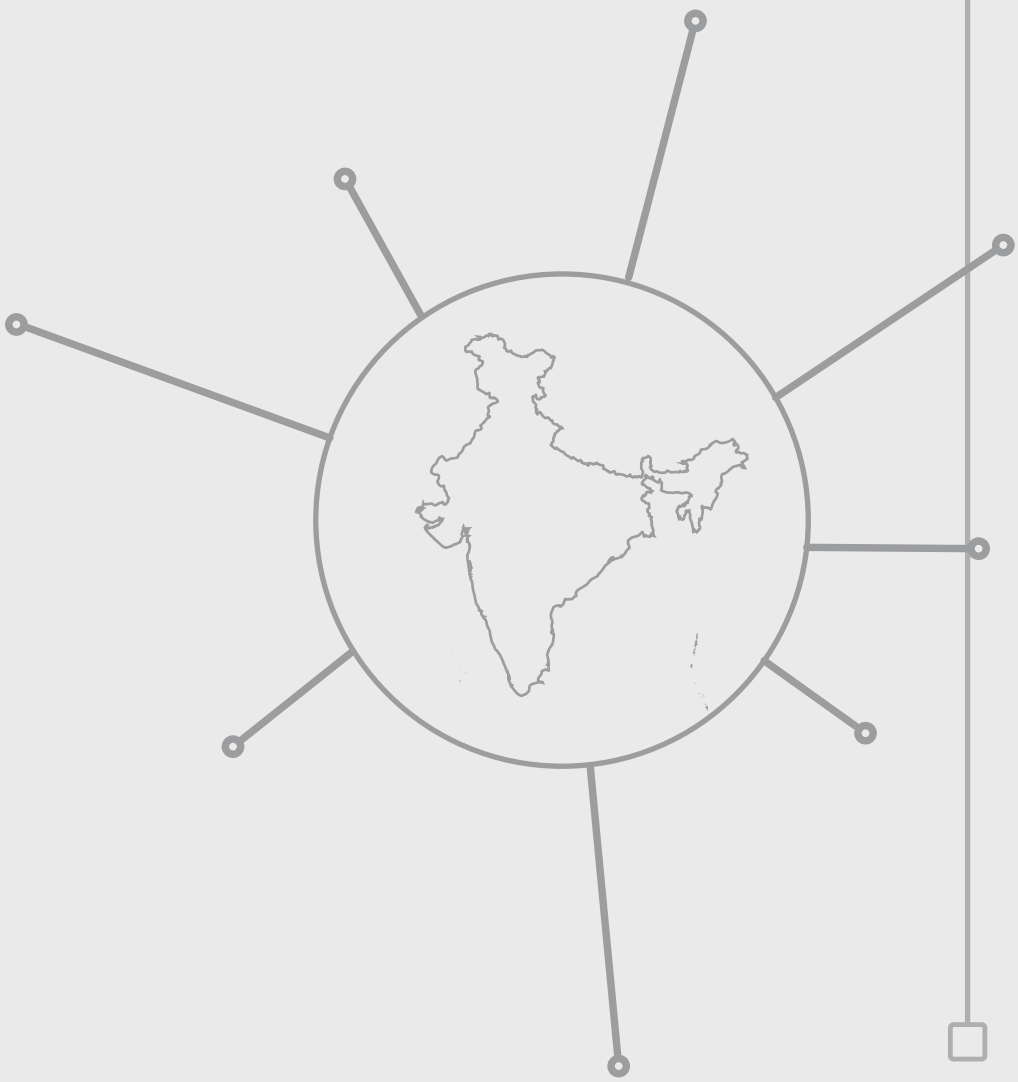
(1) Having regard to the nature, scope, and purpose of personal processing data undertaken, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, the data fiduciary and the data processor shall implement appropriate security safeguards including—

(a) use of methods such as de-identification and encryption;
(b) steps necessary to protect the integrity of personal data; and
(c) steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data.

(2) Every data fiduciary and data processor shall undertake a review of its security safeguards periodically as may be specified and may take appropriate measures accordingly.

CHAPTER 9

TOWARDS MAKING INDIA A BIG DATA CENTRE HUB



9.1 Introduction

A protectionist data protection framework opposing trans-border data flows and limiting on the progress of big data analytics will slow down the digital economy growth of our country. On the other hand, policies of allowing private companies and industry to have control over data without any regulations are also not ideal. Moreover, it is not an easy choice between the two. Going either end of the spectrum can be daunting for any economy. Which is why there has been ample talk of finding a middle ground when it comes to data flows. An approach that balances power between the public and private sectors while keeping consumer consent and safety at the heart of it.

The existence of the middle ground is debatable. However, our approach to reaching it should be more explicit. This chapter argues that instead of trying to balkanize the internet through cross-border data flows, India should harness their power by becoming a leader in the 4th industrial revolution. The years to come are an excellent opportunity to bank and excel on the IT front. India today is a hub for outsourcing services (how much is outsourced to India) Precisely because of how cost-effective and efficient the availability of services is. In a similar vein, a look at our neighbour, China makes it evident that they have excelled at manufacturing. (how much is manufactured in China). Investment in data centers today can make India the dominant force in data storage and a viable option for foreign direct investment shortly.

Designing a long-term plan to lead data storage services implores us to ask the question of why this investment is needed, the answers to them have been explored throughout this study. There are broadly two answers to why a pro-data center approach would be beneficial to India. The first of which has to do with strategic implications. Having a dearth of data centers in India would make sense on a strategic level. Getting giants such as Facebook, Amazon and, Google place there centers here could provide India with leverage in a hostile trade environment. With the US approaching trade more unilaterally than ever before, it would be a welcome boon to have some leverage over a commodity as valuable as data.

Secondly, investing and incentivising building of data centers in India would pay off dividends to the economy in more ways than one. The influx of data center solutions in India would create more jobs in the IT sector and would be a step towards improving the consumer experience. It would allow companies to place their data near to their users, a large mass of who exist in India. Also, companies that haven't already expanded their operations into India would have more of a reason to do the same if their server is located here. It would be a step in the right direction for the current administration which has pushed to make India better at ease of doing business. (where India ranks now and how this could change that)

In addition to that, data servers could lure investment in renewable energy. Large data storage facilities require vast amounts of energy to sustain. Not all of which can be sustained by fossil fuels. Incentivising more private businesses, domestic and international, to set up renewable energy plants in India would be better for India’s renewable energy sector and can provide more push for development in the same.

Answering the why on why India should invest in being a leader in data storage and big data analytics brings us to the how. The chapter will

outline sectors of data storage plants that need to be incentivised or changed to compete with international standards. This will include but will not be limited to elements such as infrastructure, broadband issues, regulatory and policy hurdles.

The cost of setting up physical data servers is high due to hardware purchases and import taxes. Once set up, the operational cost is significantly low than what the companies incur while operating them at developed cities such as London or Hong Kong.

A country's geopolitical situation becomes a vital factor for companies while considering a significant infrastructure investment. The lesser the threat perception, the attractive a country becomes as a destination for investments in data centers.

The Data Center Risk Index Report for 2016 ranks established and emerging locations according to risks affecting data center operations. The report findings suggest that the cost of setting up server farms in Brazil is at $60.9 million. While the said cost is $51.2 million in Chile and $43 million in the US, India has been recognized as one of the riskiest countries for setting up and operating data centers. In a separate report, an Indian technology services company stated (in its IPO offer document) that the estimated cost for purchasing equipment to establish a Tier-III data center in an exclusive economic zone would be INR 752 million (approximately USD 103.8 million). The actual cost would, of course, be a multiple of this amount, to account for costs related to land and statutory expenses (the document estimates the total expense at over INR 3.5 billion, i.e., approximately USD 0.5 billion), and once established, ongoing operational and maintenance charges.

9.2 Developing India as a hub for Data Centres

Various elements go into building a data center within a bureaucratic country such as India. Most of these elements can be categorised into these categories-(*)

Policy and Regulation
Infrastructural Needs

9.2.1 Policy and Regulation

If India is to develop into a market for viable data centers, the change must begin through policy reform. Presently, multiple sectors within the policy arena need to be changed to facilitate data center setups. There are tax incentives that need to be defined, so do licensing terms for data centers, along with a need to set standards for data protection and privacy. These challenges/opportunities will be discussed in detail below.

9.2.1.1. Tax Incentives

Tax rates play a crucial role in companies determining where to set up data centers. While friendly regulation will attract more investment, stringent and complex policy will have the opposite effect.

So much importance is placed on taxes because data centers are capital intensive investments that have a huge upfront cost supplemented by high maintenance costs. Among a wide range of taxes, a data center must pay property taxes, sales taxes, taxes for utilities like electricity as well as import duty for the materials sources from abroad. These taxes total to a significant amount of money and full or partial exemption from the same can go a long way to being a deciding factor. Administrations have been known used this leverage to their benefit. Nebraska came out with policy incentives for data centers that invested upwards of $200 million and created more than 30 permanent jobs (contractual and temporary jobs excluded). They did the same for data centers that garnered lower investment prospects with ‘carrots’ for a lower investment bar of $37 million.[150]

India adopting a similar approach will go a long way in incentivizing data center creation within domestic borders. It is bound to be a big plus to the country's ‘Ease of doing business' portfolio.

9.2.1.2 Existing Regulatory Framework

Tax regulation aside, another policy process that needs to be simplified is the regulatory regime that currently exists in India. The framework for data centers is outdated. Last updated in 1999, data service centers fall under a broad spectrum of Other Service Providers (OSPs) along with call centers, telemedicine as well as e-commerce.[151] This matters because OSPs are required to register with the Department of Telecommunications, which can be quite a cumbersome process. For instance, if a company wants to set up multiple data centers on the same network (which is likely to be the case), they would have to get approval separately for each one. This increases the chances of bids being rejected and can be a hurdle in the long-term plan of companies. Furthermore, DOT also has the power to change terms of registration and can arbitrarily withdraw licenses citing ‘public interest.'

There are other regulations related impediments too, such as the obligation to record calls handled by the systems at data centers for the access of security agencies, if they so wish (). This is a significant problem for

companies which strive to maintain consumer privacy. To make matters worse, the term security agencies is also loosely defined, which means that records can be screened at the beck and call of any high-level government officials.

This regulatory regime exists in tandem with the constant government oversight in the name of law enforcement. As outlined by the recommendations of the Srikrishna Committee Report and the recently auctioned RBI circular. Time and again the Indian government has attempted to get 'unfettered' access consumer data. This goes against the promise of privacy the companies seek to deliver to their consumers. This is not to say that the government has not made an effort to ensure consumer and citizen rights. The recent supreme court verdict about Section 66 of the IT act was a step in the right direction. However, it would take more such milestones to progress towards a truly 'Digital India' that places its bet on data.

Evaluating the bigger picture, the regulations stated above are but few of the numerous regulatory mechanisms that hinder ease of business in the country. Such frameworks make it difficult for the industry to operate and flourish while putting on show the lack of confidence the government has in the sector. If India is to become a global host for viable data centers, these regulations need to be relaxed. The government needs to be transparent in displaying cohesive intent, and the registration rules should be revised keeping in mind the facilitation of the growth of data service centers.

9.2.1.3 A framework for Foreign Direct Investment

Developing a data center environment in India would prove to be a magnet for inward foreign direct investment. Not least because this is a sector that is far from saturated. According to a report by the global market for data centers is expected to grow into a $155 billion industry. Out of which, the Indian market is projected to account for 4.5%.[152] This is in the best interest of the small and medium enterprises that are on the rise in India. At the time of writing, India leads globally in the number of SMEs at 42.5 million.[153] Most of these enterprises and banks use data center services to develop and deliver their services. It is essential to bank on this climate now as global stakeholders in e-commerce, and IT looks to India to expand.

According to the Wall Street Journal just opening up 100% FDI in telecom sector is not sufficient and will not be able to attract the needed $10 billion as the government expects.[154] Steps must be taken to facilitate a better spectrum and ensure competitive pricing for the same. Government stakeholders including the RBI and TRAI should cohesively come up with a framework to ensure facilitation of the anticipated inward FDI as the opportunities in the sector continue to develop.

9.2.1.4. Developing standards of adequacy for data centers

While it is essential to enable foreign and domestic stakeholders to set up data service centers in India, it is equally important to ensure that they maintain the quality of those centers. Moreover, in all fairness, it should be expected of companies to maintain the quality of these centers for two main reasons. The first among which is to ensure the best possible consumer experience. Secondly, because data centers are an expensive business and shortages in quality of infrastructure can and should be punished severely. A lot rides on the data being stored in servers, which is why private firms are expected to maintain excellent levels of security.
Regardless, there is a need for regulation that lays down quantifiable standards of adequacy

for data centers. Foreign states have recognized the need for the same. For instance, the Telecommunications Industry Association (TIA) in the US is well equipped for the purpose. Having been accredited by the American National Standards Institute (ANSI), it published requirements for data centers in 2005. The requirements are quantifiable and outline four tiers of data centers. This allows for objective monitoring of the quality of data centers.[155]

A similar tier-based method is used by Germany where certifications are doled out and renewed periodically. Similarly, India needs to establish quantifiable standards for monitoring and evaluation of data centers to ensure quality.

9.2.2 Developing New and Existing Infrastructure

Discussing standards of adequacy leads us to question whether India has the required infrastructural capacity to reach and maintain those standards. A key reason why data service centers are so expensive is the number of resources that go into maintaining and running a center. India being a developing economy, would need to keep up with the unrelenting usage of energy and space required by data centers. This will focus on two main themes. Firstly, identifying what it takes to install and maintain data centers and secondly, where India stands regarding delivering those resources and services.

9.2.2.1 Electricity Requirements

Perhaps the biggest demand of data centers is the sheer amount of energy they consume. For instance, just running a data center in the US costs $510,000 a month. Out of $510,000, electricity tariffs account for $382,500 (75%).[156] As the number of data centers increases, so will the need for electricity.

Furthermore, it works in a country's favor if the tariffs on electricity are lower. While in the US the average monthly cost for running a center is $510,000, it costs almost double in Brazil ($950,000).[157] Hence, in the medium term, maintenance costs are likely to exceed the initial building costs for most data centers (7 years taking the US as the reference point). Which is precisely why companies prefer setting up data centers in places where maintenance costs (primarily energy) are cheaper.

However, in the case of India, the cost of electricity is secondary as compared to its availability. It is no secret that India has unmet energy needs. Estimates show that almost 25% of the population does not have access to electricity.[158] With limited infrastructure such as this, it would be a challenge to support data centers.

Moreover, if somehow the energy needs were met, it would take significantly longer to pass through the bureaucratic red tape to utilize the energy. A report by IAMAI claims that it would take almost two months on average to go through 7 different policy hurdles to get a working electricity connection. In contrast, it would only take three days in Japan.

For India to become a hub for data storage and analytics, it is fundamental to relax on such regulations, extend the energy grid using renewables and develop well-marketed incentives to portray the same.

9.2.2.2 Cooling requirements

Data centers consume enormous amounts of energy, because of which they produce heat. This requires cooling down for functioning, and the requirements for this can be huge.
1,362,748 liters of water go into the daily functioning of a 15-megawatt data center. As the size and number of such centers increases,

so makes the demand for water.[159]

India has been trying to cope up with this demand. According to a study by IAMAI, Nalco developed an onsite mobile unit with all ancillary piping, pumps, controls and, tankage to support the main technology components of an ultra-filtration program followed by reverse osmosis for a data center facility in Bangalore which reduced water consumption by 164,250,000 liters annually.[160]

Even with engineering solutions, water supply will still be a challenge for India if it is to become a hub for data centers. The Independent claims that 200,000 people in India die because of water scarcity. A report by the government think tank, NITI Aayog says that India's demand for water will be double that of the supply by 2030.[161] In a time where water is in such extreme shortage, it is unthinkable to allocate millions of liters to data centers.

Water and electricity are but two of the requirements for setting up data centers. There are other factors involved too, such as the sufficient availability of land and the capacity of structures to avoid natural and human-made disasters. These are areas where India will have to look for solutions to become a major player in data center hosting. In addition to meeting resource-based challenges, it is also imperative that India is able to provide the technical facilities for centers to operate through allocating sufficient space on the spectrum with appealing cost and quality options.

9.2.2.3 Broadband Issues

India does not rank favorably in broadband penetration as well as internet usage. As of December 2015, 30.91% of India had wireless broadband (371 million people).[162] Part of the reason why India has not been able to achieve better penetration is the size of the country. Other developing (and developed) countries have flourished under this area such as Singapore because of their relatively smaller size, which makes it easier to ensure connectivity.

In addition to limited coverage, the internet services available are not up to scratch concerning speed. India has the lowest average internet in the Asia-Pacific region.
Lack of internet coverage makes it harder for data centers to function as they rely on cheap and quality internet bandwidth. The most

(*)*"2016 Conducive Policy and Regulatory Environment to incentivise data center infrastructure."*
https://cms.iamai.in/Content/PolicyPapers/7065f212-0eb7-4a05-a1aa-3bc9433eb75f.pdf
Accessed 24 Oct. 2018
[150]"*Impact of Taxes & Incentives on Data Center Locations - DocPlayer.net.*"
https://docplayer.net/5244400-Impact-of-taxes-incentives-on-data-center-locations.html. Accessed 14 Nov. 2018.
[151]"*New Telecom Policy 1999 (India) - unpan1.un.org, 24.07.2012.*"
http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan040889.pdf. Accessed 14 Nov. 2018.
[152]"*India's data centre market to reach $4.5 billion by 2018: IAMAI ....*" *26 May. 2016,*
https://telecom.economictimes.indiatimes.com/news/indias-data-centre-market-to-reach-4-5-billion-by-2018-iamai/52443770
. Accessed 14 Nov. 2018.
[153]"*SME Sector in India – Statistics, Trends, Reports – EVOMA.*"
https://evoma.com/business-centre/sme-sector-in-india-statistics-trends-reports/. Accessed 14 Nov. 2018.
[154]"*Telecom Sector Needs More Than FDI - India Real Time - WSJ.*" *18 Jul. 2013,*
https://blogs.wsj.com/indiarealtime/2013/07/18/telecom-sector-needs-more-than-fdi/. Accessed 14 Nov. 2018.
[155]"*About Data Centers - TIA-942.org.*" *http://www.tia-942.org/content/162/289/About_Data_Centers. Accessed 14 Nov. 2018.*
[156]"*Build Or Buy? The Economics Of Data Center Facilities - Data Centers.*"
https://www.io.com/wp-content/uploads/2014/10/WhitePaper_Forrester_Build-or-Buy_Economics-of-Data-Center-Facilities.p

significant deterrent hampering the growth of India's data center and cloud computing industry is the lack of sufficient infrastructural support required to set up and operate centers in tier II and tier III cities. A mandate for data localization might create a harsh environment for critical industries that contribute significantly to India's digital as well as economic growth.

df. Accessed 14 Nov. 2018.

[157] *"Brazil Legislators Bear Down on Internet Bill - Wall Street Journal." 13 Nov. 2013, https://www.wsj.com/articles/brazil-legislators-bear-down-on-internet-bill-1384384450. Accessed 14 Nov. 2018.*

[158] *"Living in the Dark: 240 Million Indians Have No Electricity - Bloomberg." 24 Jan. 2017, https://www.bloomberg.com/news/features/2017-01-24/living-in-the-dark-240-million-indians-have-no-electricity. Accessed 14 Nov. 2018.*

[159] *IAMAI. (2016). Make in India: Conducive Policy and Regulatory Environment to Incentivize Data Centre Infrastructure [Ebook] (pp. 2-30). IAMAI.*

[160] *IAMAI. (2016). Make in India: Conducive Policy and Regulatory Environment to Incentivize Data Centre Infrastructure [Ebook] (pp. 2-30). IAMAI.*

[161] *"India's 'worst water crisis in its history' is only going to get worse ...." 17 Jun. 2018, https://www.independent.co.uk/news/world/asia/india-water-crisis-shortage-niti-aayog-report-drought-mismanagement-a8403286.html. Accessed 14 Nov. 2018.*

[162] *"Internet usage in India - Statista." https://www.statista.com/topics/2157/internet-usage-in-india/. Accessed 14 Nov. 2018.*

9.3 Enabling Domestic Big Data Industry

The data analytics market in India is growing at a fast pace, with companies and startups offering analytics services and products catering to various industries. Different sectors have seen different penetration and adoption of analytics, and so is the revenue generation from these sectors.

Analytics, data science and big data industry in India is currently estimated to be $2.71 billion annually in revenues, growing at a healthy rate of 33.5% CAGR.[163] It is expected to grow seven times in the next seven years. It is estimated to become a 20-billion dollar industry in India by 2025.[164] Chart 2 below depicts the revenue generated (in $ bn) in the analytics industry from 2016 to 2018. The projected revenue in 2025 is expected to be more than $20 billion.

Post-1991, the information technology (IT) and Business Process Outsourcing (BPO) industries became the go-to places for youth in India looking for a better life. In fact, India has one of the fastest growing service sectors in the world with an annual growth rate above 9% since 2001.[166] India now faces a two-forked problem – scores of graduates who need to be skilled in technologies that companies want to hire and millions of professionals with skill sets that are becoming redundant at a rapid pace who need to upskill. Around 40 percent of IT professionals in India need to upskill themselves over the next few years while 48 percent of Indian employers report difficulties filling job vacancies due to talent shortages.

Data science is the fastest-growing field in India. Currently, India has over 50,000 open data analytics jobs, and this is expected to

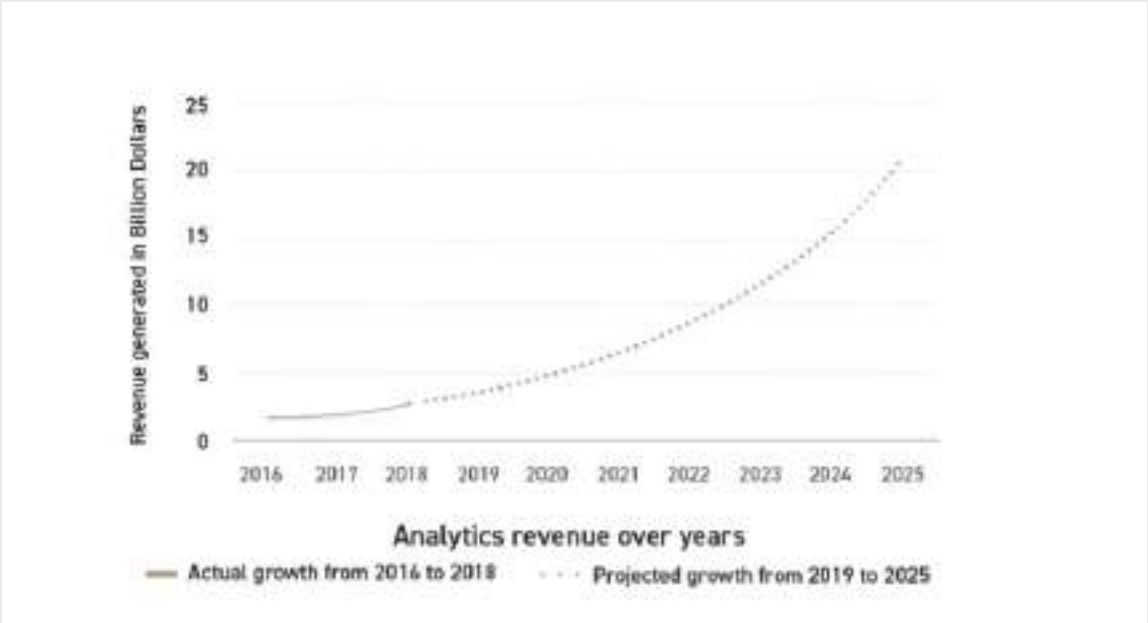


Chart 2: Revenue generated (in $ bn) in analytics industry and the projected growth in the next 6 years[16]

grow to 100,000 in 2018.[167] According to a staffing solutions company, TeamLease Services, India will face a demand-supply gap of 2 lakh data analytics professionals by 2020.[168] This lag between demand and supply exists not only in India but is a global phenomenon. As per the estimates of McKinsey, the gap between supply and requisite demand for analytics skills in the US will reach 50-60% by 2018.[169]

[163] *"Analytics & Data Science Industry In India: Study 2018." 18 Jun. 2018, https://www.analyticsindiamag.com/analytics-data-science-industry-in-india-study-2018-by-analytixlabs-aim/. Accessed 14 Nov. 2018.*
[164] *"Industry Study 2018_Final_18 June - Analytics India Magazine." https://www.analyticsindiamag.com/analytics-data-science-industry-in-india-study-2018-by-analytixlabs-aim/?aid=25498&sa=0. Accessed 14 Nov. 2018.*
[165] *https://www.analyticsindiamag.com/analytics-data-science-industry-in-india-study-2018-by-analytixlabs-aim/*
[166] *"India Economy Indian Economy, business opportunities in India ...." https://www.globaltenders.com/economy-of-india.php/. Accessed 14 Nov. 2018.*
[167] *"Big data, machine learning, AI to shape job market in 2018 - The ...." 31 Dec. 2017, https://www.thehindubusinessline.com/info-tech/big-data-machine-learning-ai-to-shape-job-market-in-2018/article10006991.ece. Accessed 14 Nov. 2018.*
[168] *"The Great Indian Big Data Talent Gap - Great Learning." 10 Apr. 2017, https://www.greatlearning.in/blog/the-great-indian-big-data-talent-gap/. Accessed 14 Nov. 2018.*
[169] *"Department of Defense Accomplishments | Belfer Center for Science ...." https://www.belfercenter.org/publication/department-defense-accomplishments. Accessed 7 Nov. 2018.*

CHAPTER 10

COMPARATIVE ANALYSIS WITH OTHER NATIONS

10.1 Indonesia

Indonesia enacted its law on data localization in 2012 under through government regulation No. 82 on the Implementation of Electronic Systems and Transactions (also called the GR82). This enactment had a transitional provision of 5 years for existing electronic system operators (defined to mean any person, state entity, business entity and community that provides, manages and/ or operates an Electronic System whether independently or collectively for an Electronic System user for its own use and/ or another party's use) to comply with the regulations. However, this transitional period of 5 years turned out to be insufficient for electronic system operators to adapt to the localization requirements.[170]

Under the GR82, these operators providing public services were required to have data centers (including data recovery centers) inside Indonesia by October 2017. It is noteworthy that the term “public services” has not been defined under GR 82.[171]

Towards the end of the five-year transitional period of the GR 82, the business community advocated with the government for diluting, inter alia, the data localization mandate. The Ministry of Communication and Information Technology indicated that it would amend the GR 82 and provide leniency concerning the onshore data center and disaster recovery requirements. Under this draft amendment, there is no longer a requirement for electronic system operators who provide public services to have data centers and disaster recovery centers inside Indonesia under all circumstances. However, such electronic service providers will still be required to process and store "strategic electronic data."[172] Moreover, have disaster recovery centers for such data inside Indonesia.

To sum, in view of the pushback by the industry in relation to data localization and other data privacy mandates, the government of Indonesia has proposed an amendment to the GR 82 that is expected to be more liberal on the data localisation mandate and at the same time, provide an unambiguous regulatory ecosystem for businesses.

[170] *"Indonesia Telecoms and Media – Getting The Deal Through – GTDT." https://gettingthedealthrough.com/area/39/jurisdiction/42/telecoms-media-indonesia/. Accessed 15 Nov. 2018.*

[171] *"Public services" has been defined under a separate Public Services Law, however, to mean activities for the purpose of fulfilling goods and services needs for every citizen and resident in accordance with the laws and regulations*

[172] *Will be defined under the proposed amendment to the GR 82 as data that strategically affects the public interest, public services, the continuity of the State's administration, or the State's defense and security. E.g., intelligence data, population data or Indonesian citizens' data, and state defense and security data.*

10.2 Vietnam

Vietnam adopted its Law on Cybersecurity in June 2018, and it will come into effect from January 1, 2019. Under the new law, all cyber activities in Vietnam shall be within the controls of the Ministry of Public Security.
Article 26.3 of the Law on Cybersecurity mandates the local storage of data by certain entities. This mandate applies to entities, both foreign and domestic,[173] which:

a) provide telecom, internet and value-added services on the cyberspace in Vietnam; and

b) are involved in the collection, exploitation, analysis, and processing of personal information, data about users' relationships and data generated by users in Vietnam.

Foreign companies falling within the scope of the above are required to have a physical presence in Vietnam through a branch office or a representative office.[174]

Article 26.3 of the Law on Cybersecurity states that the following information is required to be stored in Vietnam for a duration of time (not specified yet):[175]

a) personal information;
b) data about users' relationships; and
c) all other data generated by users in Vietnam.

However, it is as yet unclear whether the above categories of data are required to be stored exclusively in Vietnam. This is because:

a) the above provisions could be interpreted to imply that a copy of the above data is required to be stored in Vietnam, while another copy is stored overseas, and the copy stored in Vietnam can be deleted after the statutorily specified time; or
b) it could also imply that the above data be stored exclusively in Vietnam for the statutorily specified duration of time subsequent to which, it may be stored overseas.

This new law gives the government greater control over foreign digital groups as well as over local users who post anti-government propaganda or information that "ignites violence and disturbs public security, or defamatory and slanderous content."

[173] *"Draft Decree to implement Cybersecurity Law doesn't dampen ...." https://www.lexology.com/library/detail.aspx?g=0d3f8017-8849-45db-b5d0-6947b790755f. Accessed 15 Nov. 2018.*
[174] *"Doing Business in Vietnam - PwC." https://www.pwc.de/de/internationale-maerkte/assets/doing-business-in-vietnam.pdf. Accessed 15 Nov. 2018.*
[175] *"Vietnam National Assembly Passes the Law on Cybersecurity - Lexology." 15 Jun. 2018, https://www.lexology.com/library/detail.aspx?g=843a0ed4-5583-434f-8f56-fc206f14c770. Accessed 15 Nov. 2018.*

10.3 European Union

Introduction

The GDPR, i.e. General Data Protection Regulation (REGULATION (EU) 2016/679), adopted on May 27th, 2016 and came into force after a two-year transition period on May 25th, 2018 replaces the Data Protection Directive (DPD 95/46/EC). The Regulation (EU) 2016/679[176] is an essential step to strengthen individuals' fundamental rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital single market.

The General Data Protection Regulation in EU law is an overhaul framework on privacy for all (EU) and the European Economic Area (EEA) citizens. It addresses the export of personal data outside the EU and EEA areas and gives controls to citizens over thier personal data simplify the regulatory environment for international business by unifying the regulation within the EU.[177]

The Data Protection Law Enforcement

Directive (EU) 2016/680[178] Protects citizens' fundamental right to data protection whenever personal data is used by criminal law enforcement authorities for law enforcement purposes. It protects the personal data of people of all kinds - victims, witnesses and suspects, and duly facilitates overseas cooperation in the fight against crime.
It came into force in May 2016.

National data protection authorities

EU countries have set up national bodies responsible for protecting personal data in accordance with Article 8(3) of the Charter of Fundamental Rights of the EU.[179]

[176] *https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=CELEX:02016R0679-20160504&qid=1532348683434*
[177] *"The GDPR - European Commission - Europa EU." https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf. Accessed 15 Nov. 2018.*
[178] *eur-lex.europa.eu/legal-content/EN/TXT/?uri=uris-erv%3AOJ.L_.2016.119.01.0089.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC*

[179] *"EUROPEAN COMMISSION Brussels, 10.1.2017 COM(2017) 8 final ...." 10 Jan. 2017, https://ec.europa.eu/newsroom/document.cfm?doc_id=41158. Accessed 15 Nov. 2018.*

10.4 Japan

Japan recently amended its data protection law, Japan's Act on the Protection of Personal Information in May 2017. This amendment significantly changed the rules around the collection, storage and transfer of personal information. These new amendments appear to put Japan's data protection jurisprudence at par with EU's GDPR, which generally proscribes the transfer of personal data outside the EU to any nation perceived as having an adequate level of data protection. The new amendments provide stronger foundations for data protection domestically and create unambiguous centralised rules on cross-border flow of data concerning Japanese citizens.

Japan also happens to be a member of the Asia-Pacific Economic Cooperation (the APEC), an economic forum established in 1989 comprising 21 economies including Australia, China, Indonesia, South Korea, Russia, and the USA. APEC has a voluntary system of Cross-Border Privacy Rules in place. This system allows, on one hand, privacy and data protection needs in individual members, but on the other hand, it balances these needs against cross-border flows of information that facilitate technology sharing and progress.[180]

This ensures that participating members comply with domestic law protection requirements at the very least, and may adopt higher standards if they so wish. Currently, only Japan, Canada, Mexico, and the USA participate. Certification of compliance with this system is a good way for participating businesses to establish the requisite systemic protections concerning the cross-border flow of data.

Naturally, companies that are certified to be compliant with the APEC's Cross-Border Privacy Rules, will be deemed to be qualified under the statutory law for providing acceptable levels of data protection. These growing sentiments are positively supporting Japan's goal to secure the freedom of cross-border data transfers and to unify the regulations of data protection policies across countries.[181]

[180] *"About APEC - Asia-Pacific Economic Cooperation." https://www.apec.org/About-Us/About-APEC. Accessed 15 Nov. 2018.*

[181] *"Japan, EU Launching High-Level Talks on Safe Data Transfers," Nikkei Asian Review, accessed October 21, 2018.*

10.5 Brazil

Currently, Brazil does not have a laid-down enactment concerning the protection of personal data. The Ministry of Justice, however, has been in the process of drafting the Law on Data Protection since 2011. Several rounds of consultations and discussions later, the Bill has been sent to the House of Deputies where it is expected to receive positive confirmation and be enacted into law. The absence of specific legislation does not, however, preclude action under Brazilian law for any breach of fiduciary obligations about the protection of personal data.[182]

The Federal Constitution which envisages privacy protection as a fundamental right, the Brazilian Civil Rights Framework for the Internet which regulates aspects of the protection of personal data processed online by connection providers and by internet application providers, the Consumer Protection Code, the Compliant Debtors List Act and a few others envisage the protection of personal information in some form or the other. These laws apply to Brazilian persons (individuals as well as body corporates) as well as residents of Brazil. The Civil Rights Framework for the Internet operates to the collection, storage, retention, treating and communication of personal data by connection providers and internet applications providers, when at least one of these takes place in Brazil.

The Bill of the Data Protection Act, however, foresees a broader jurisdictional scope and, if enacted in the form it currently reads, will apply to the following categories:

a) Any data processing taking place in Brazil;

b) Any data processing operation whose purposes are the offer of goods or services in Brazil;

c) Any data processing operation referring to data subjects in Brazil; and

d) Any data processing operation is referring to data collected in Brazil.

The Bill also proposes to have an entire chapter dedicated to the international transfer of data. Article 33 of the Bill establishes that an international transfer would only be allowed if provided to countries with equivalent levels of data protection or when expressly consented by data subjects after specific information concerning the international nature of the operation and the risks entailed has been given. The Bill also contains a limited number of exceptions and sets out a joint liability between assignors and assignees for any data treatment occurred after the transfer.[183]

The Civil Rights Framework for the Internet, which is currently the law in force, allows the storage of subjects' personal data anywhere. However, under Article 11, it provides that the applicability of the Framework extend to data processing if such data was collected in Brazil, even if it is stored abroad. The Bill of the Data Protection Act envisages creating a data protection authority to approve the international transfer of data.
The Privacy Act does not explicitly define "serious harm," but the Office of the Australian Information Commissioner (OAIC) defines this as: "may include serious physical, psychological, emotional, financial, or reputational harm." This is helpful, it is not clear who makes the determination, but the data subject or the company that was breached.

[182] *"Brazil's New Data Protection Law: The LGPD - Mondaq." 19 Sep. 2018, https://bit.ly/2zbWpqT Accessed 15 Nov. 2018.*
[183] *"Data protection in Brazil: overview | Practical Law - Westlaw." https://bit.ly/2Ftbmuj Accessed 15 Nov. 2018.*

CHAPTER 11

SECTORAL ANALYSIS

11.1 Introduction

In this chapter, we analyse four critical sectors that are dependent on the free flow of data across the border and how data localisation policies may hurt their growth in the long term. We have also analysed case studies that have benefited with cross-border data flow and to demonstrate the need for cross-border exchange of data.

India's digital and startup ecosystem depends tremendously on cross-border data flows.[184]

- Zoho Corp based out of Chennai operates out of data centers in California and New Jersey.[185]
- Myntra and redBus have been hosting their servers with global cloud providers.[186]
- Flipkart depended on data centers in Canada for its early operations.[187]
- Fortis Healthcare has migrated from its own corporate data center to an outsourced cloud service provider that led to cost savings and remote healthcare service delivery.

[184]"2018 The Economics of Data Flows in Asia Pacific." http://www.asiacloudcomputing.org/research/2018-research/2018-the-economics-of-data-flows-in-asia-pacific. Accessed 16 Nov. 2018.
[185]"12 Best Zoho Products: Reviews Of The Most Popular Services ...." 9 Nov. 2018, https://financesonline.com/top-zoho-products-reviews-popular-services/. Accessed 14 Nov. 2018.
[186]"Should You Choose a Cloud or On-Premise E-commerce Platform?." http://www.netsuite.com/portal/resource/articles/ecommerce/should-you-choose-cloud-on-premise-ecommerce-platform.shtml. Accessed 14 Nov. 2018.
[187]"Microsoft nabs Indian e-commerce giant Flipkart for Azure as cloud ...." 20 Feb. 2017, https://venturebeat.com/2017/02/20/indian-internet-giant-flipkart-partners-with-microsoft/. Accessed 14 Nov. 2018.

11.2 Outsourcing Industry

The outsourcing industry has been growing at 8% annually and has contributed to 2/3rds of India's GDP in the last few years. It is a crucial sector for economic growth.

From the backend call center work, the outsourcing industry has moved to services such as cloud and IoT. As India progresses in the outsourcing industry, cross-border data flows will act as a critical enabler for business growth.

Enterprises are now increasingly outsourcing data analytics processes to talent-rich, cost-efficient regions such as India. Adoption has been highest amongst telecom, banking, financial services and insurance (BFSI), and e-commerce sectors, which continue to invest and innovate with smart analytics. A vast number of industries rely on data from their locations around the world to make routine decisions. To facilitate this decision-making process and provide added value to consumers, data must flow freely across international borders.

Case Study - Market Equations

Market Equations is a research and analytics outsourcing company helping businesses solve critical problems through the application of advanced analytics. As part of the company's analytics offering, it had developed an inventory and order management predictive model for an e-commerce retailer in the UK.

The solution ensures data integrity and hygiene, conducted product clustering to study trends and patterns, analyzed product categories by sales, seasonality, and stock levels to uncover irregularities. In this regard, the cross-border nature of outsourcing business enables data flows and resource sharing between different locations globally, demonstrating the extent of collaboration and exchange of information, knowledge, and human resources.[188]

[188] *Market Equations (2017) About Market Equations, www.marketequations.com/about-us.html Accessed 14 Nov. 2018.*

11.3 Manufacturing Industry

Manufacturing is one of the biggest employer in India. With the rise of IoT and smart manufacturing, India is witnessing to implement networks of sensors and actuators for data collection, monitoring, decision-making, and process optimization.

For example, Indian Railways will be rolling out locomotives with solutions such as remote diagnostics and predictive maintenance and these trains will be part of a broader ecosystem connected to the industrial Internet. For this, remote factory management is a necessity, which would scale up the transfer of data across borders. Data localisation will cause significant challenges for the successful delivery of such services.

Case Study - Wipro Ltd.

Wipro Ltd. uses cognitive computing, hyper-automation, robotics, cloud, analytics, and emerging technologies. In the manufacturing sector, Wipro integrates intelligence with operations. Leveraging the use of cloud has allowed Wipro to focus on significant constituents of Industry 4.0, such as creating smart manufacturing environments.

Using cloud, Wipro has supported a large number of manufacturing clients across multiple jurisdictions. Cloud computing, enabled by the free flow of data, ensures that Wipro maintains cash flow while reducing operating costs and being able to innovate to compete–i.e., to move to more efficient manufacturing processes, given the price sensitivity of customers in the sector.

11.4 Financial Services and E-Commerce

India's e-commerce sector is still at a very early stage as compared to the US and Europe, while at the same time, it has excellent potential for the future. Data localisation will hurt the industry as India, much like other nations, is built on top of existing global services. Domestic companies such as Zoho (more in the case study) and Sharechat are built on servers located on Amazon Web Services and Google. Forced data localisation may lead to denial of access to international and enhanced services, as a tit-for-tat for what happens in India. The chance to global may be lost completely which may increase cost in the long run, forcing some of the businesses to exit the Indian market.

Also, since e-commerce is not a critical sector, it is unwarranted to place localisation norms in this case. The data which is collected includes the trends mostly and has minimal personal information. To secure this, localisation of data is not necessary.

As per the draft e-commerce policy, the data generated from Indian usage of e-commerce platforms must be localised. By and large, it puts this data in charge of the Indian government for "national security and public policy" objectives. The Justice Srikrishna committee also recommended the localization mandate for e-commerce data. The committee's rationale was more toward preserving the integrity of Indian users' privacy. However, the Committee's report lacks clarity on the economic ramifications and the infrastructural costs associated with localization, including the setting up of indigenous data centers. This clarity was sought to address in the e-commerce draft policy through a unique structure of direct and indirect tax incentives as well as prioritising the development of data centers as critical infrastructure. The draft proposes a "cooling-off period" of two years before data localization becomes mandatory.

11. 5 Healthcare Industry

Cross-border data flow is critical to the healthcare industry in India. A high number of service providers are now using cloud infrastructure so that doctors can access data from anywhere. This helps in providing real-time solutions. It has brought down the cost of operations that has resulted in the rise of medical tourism, attracting patients to India from all around the world and subsequently adding to India's GDP.

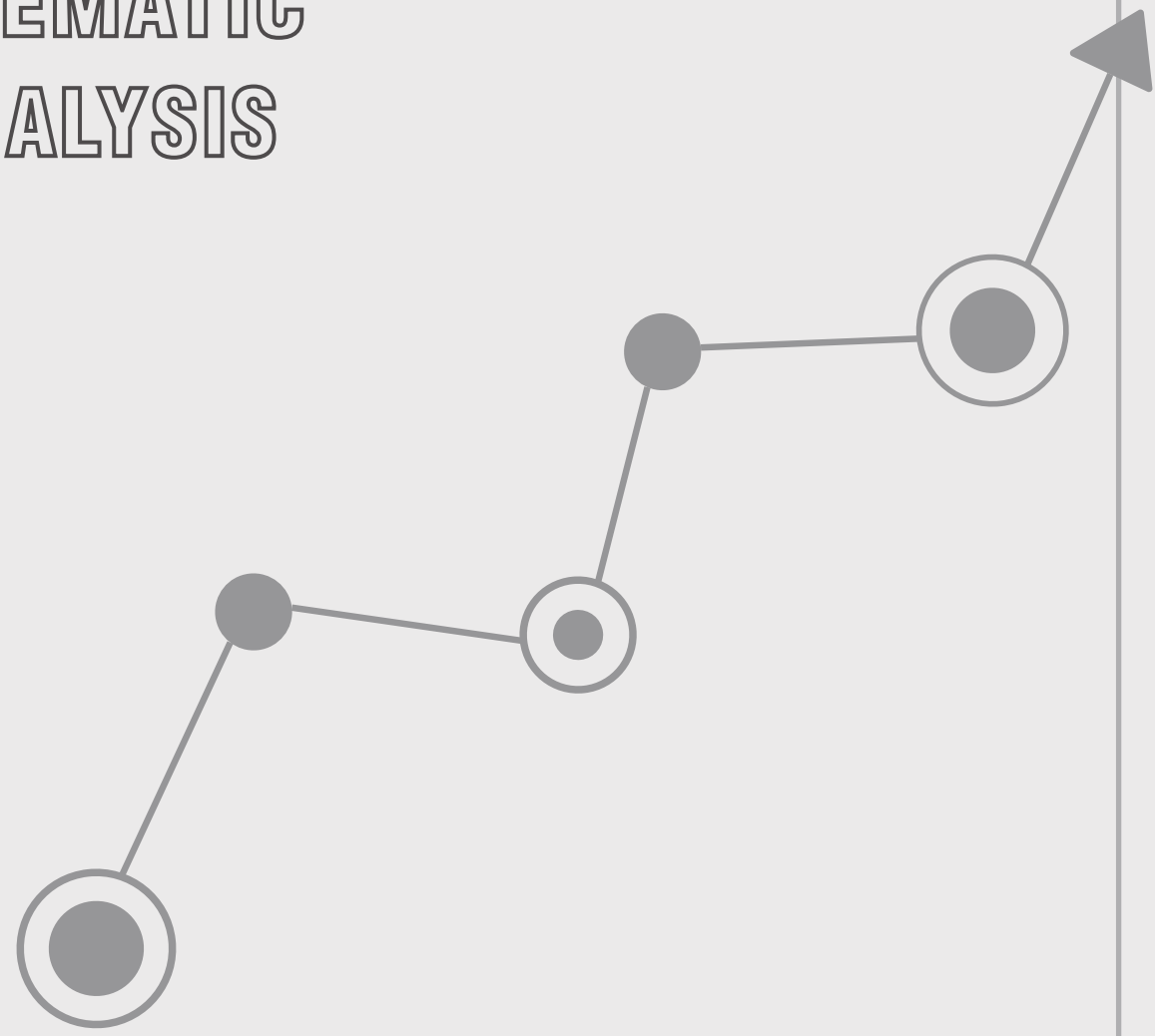
Case Study: Healthy

Healthy is a medical tourism start-up in India, which utilizes data-intensive research to deliver cross-border patient care. The free flow of data and the flexibility of cloud technology allows Healthy to access the latest information and resources in order to provide new and improved experiences for customers and patients.[189]

[189] *Imarticus Learning and NASSCOM (2017) Analytics Employment Landscape in India, https://imarticus.org/wp-content/uploads/2017/04/Industry-Report-Analytics- 2017.pdf Accessed 14 Nov. 2018.*

CHAPTER 12

CONTENT AND THEMATIC ANALYSIS



12.1 Introduction

Conducting primary and secondary research around data localisation involved processing inputs gathered through a shared questionnaire (presented in the methodology section) as well as documents received from industry and civil society. These inputs have been instrumental in informing our understanding on localization. A key feature of these inputs were the sources they were collected from. The documents and responses to the designed questionnaire came from three main areas, civil society, academia, and industry.

This gave us the perfect platform to quantify and examine where each of these sectors stood in terms of different aspects of localisation. The study analysed the inputs using a content analysis and thematic analysis to derive insights from these inputs which are presented in the sections below.

12.2 Methodology

The methodology developed for the paper was built through the qualitative inputs received through interaction with members of industry, academia, government, and civil society. The team reached out to professionals through two methods. Firstly, a questionnaire developed with 13 questions regarding localization and its impact on the economy, security, prospects of growth, and possible alternatives available. Secondly, the team reached out to high-level officials through semi-structured interviews to get their inputs on the subject.

The questionnaire mentioned above formed the basis for a content analysis on subjects related to local data storage and mandatory localisation. We would like to highlight that the concept of local data storage and mandatory localisation are not mutually inclusive and may not necessarily complement each other, except for some circumstances.

The questions involved in the questionnaire are listed below:

1. Will data storage in India ease the access of information to law enforcement agencies for criminal investigation?

2. Is it possible to develop a system of voluntary cross-border transfer of data for India with other nations?

3. Will data localisation help in making Indian data more secure?

4. Will local storage help in auditing of the data processed by fiduciaries in India?

5. Is data localisation the only answer to create a vibrant digital economy?

6. Does local storage help in Improving Network Latencies?

7. Will local data storage give a level-playing field to Indian technology firms?

8. Is data transfer from undersea cables a risk to security?

9. What are the costs involved of setting up servers in India?

10. Will local storage of data and presence of data fiduciaries in India expand India's tax jurisdiction over the data processed by foreign fiduciaries?

11. Will data storage support India's Data Centre and Cloud Computing Industry?

12. Is data localisation a mandatory requirement for the growth of data center, CC and IT industry in India?

13. Will local data storage help growth of the domestic IT industry in India?

This questionnaire was distributed to civil society (comprising of a mix of lawyers, think tanks, researchers, and policy practitioners working in the space), academia (professors), and the industry (consultants, managers). The responses to these questions were analysed to observe patterns and draw conclusions regarding the view of different sectors on data localization.

12.2.1 Reliability and Coding

The responses to questions were classified into 7 categories, namely, yes, to some extent, unsure, no, to a large extent , better alternatives available, non-answer. For the sake of simplicity in quantification, these categories were assigned values from 0-6 (inclusive).

There may be concerns regarding whether or

not the analysis conducted is reliable in its results. To address the same, the responses to the questionnaire have been divided into categories depending on how concise and easily classifiable each answer is. Out of a total of 430+ responses to the questions (excluding the names and designations), ~85% (367) were sampled randomly to determine the scope of leeway in each answer. It was found that a total of 131 (~36%) answers were simple statements, being one-word multiple times (for instance, 'yes', 'no', 'not necessarily'). Similarly, the responses sampled contained 130 (~36%) one-sentence answers. The presence of short answers removes ambiguity and leeway for interpretation, making the results more reliable.

There were also quite a few longer answers (2 sentences or more). The length of these answers increased because of added explanations. For the sake of better classification, these longer have been divided into two categories, i.e., answers with summary as the first sentence, and answers without the summary mentioned in the first sentence. Quantifying the same, 91 answers (~25%) had their gist as the first sentence while only 15 (~4%) did not begin with summaries of what was to follow.

The content analysis, is thus dependable because of the concise nature of the answers across the questionnaire. The scope for interpretation exists most in answers that are long and do not begin with a summary. However, they are few and far in between. This minimizes the scope for interpretation in the analysis, making it more reliable.

12.3 Analysis and Results

The inputs recieved during the study came from experts working in different sectors with varying levels of expertise on data localisation and how it might impact the space. Leveraging that, this content analysis is an attempt to gauge how the broader community (academia, civil society, and industry) perceive localisation and its different aspects. The following section will elaborate and provide an overview of the same.

12.3.1 Question 1: Will data storage support India's Data Centre and Cloud Computing Industry?

Fig 1. Civil Society's Response to Question 1

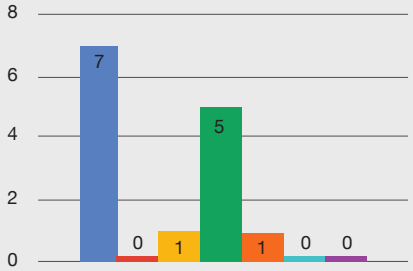


Fig 2. Academia's Response to Question 1

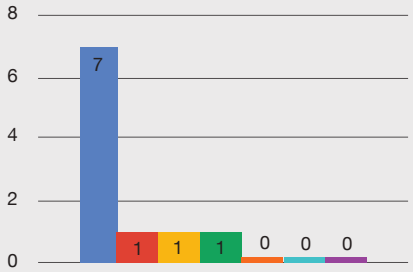
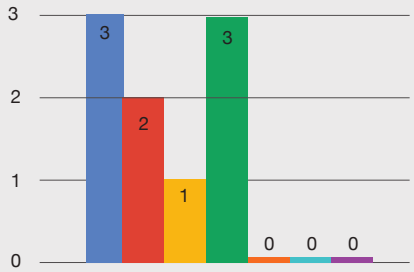


Fig 3. Industry's Response to Question 1



There is consistency between academia, civil society, and the industry regarding the idea that local data storage will support India's data centre and the cloud computing industry. Out of the 33 responses collected, ~51% believed in the idea that localization would support the data centre and cloud computing industry in India. ~27% were opposed to the idea with civil society having the largest opposer base (in relative terms) with ~35%.

12.3.2 Question 2: Is data localisation a mandatory requirement for the growth of data center industry, CC and IT in India?

Fig 4. Civil Society's Response to Question 2

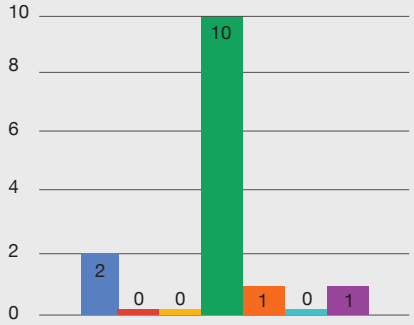


Fig 5. Academia's Response to Question 2

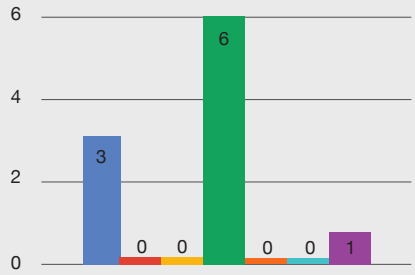
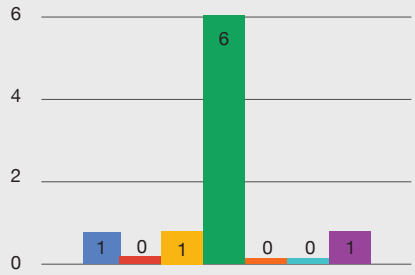


Fig 6. Industry's Response to Question 2



~66% of the Civil Society, Academia, and the Industry believe that data localisation is not a mandatory requirement for the growth of a data centre, CC and IT industry in India. Only ~18% of the respondents claimed the inverse to be the case.

12.3.3 Question 3: Will local data storage help growth of the domestic IT industry in India?

Fig 7. Civil Society's Response to Question 3

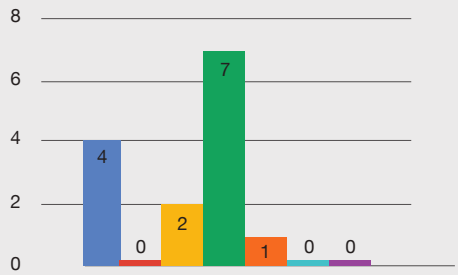


Fig 8. Academia's Response to Question 3

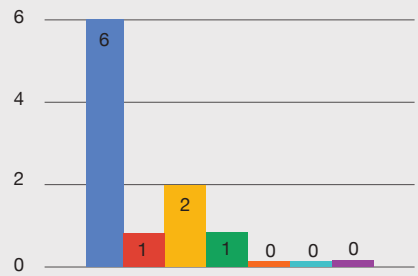
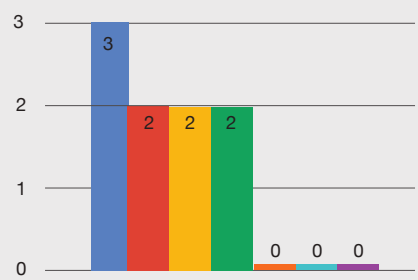


Fig 9. Indusrty's Response to Question 3



There are discrepancies between the stances of Civil Society, Academia, and the Industry when it comes to whether local data storage will help in the growth of the domestic IT industry in India. In total ~40% of the response base believes in the statement, in contrast to the 30% of those who oppose the same. Interestingly, 50% of the response base in civil society has responded no, as compared to 10% of academia and ~22% of the industry.

12.3.4 Question 4: Will local storage of data in India ease the access of Information to Law Enforcement Agencies for Criminal Investigation?

Fig 10. Civil Society's Response to Question 4

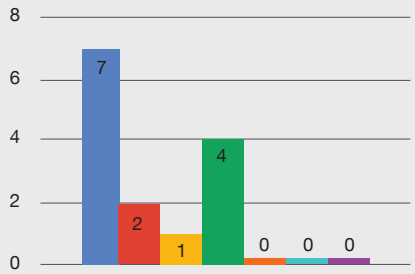


Fig 11. Acedemia's Response to Question 4

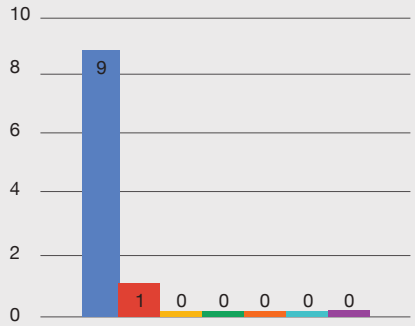
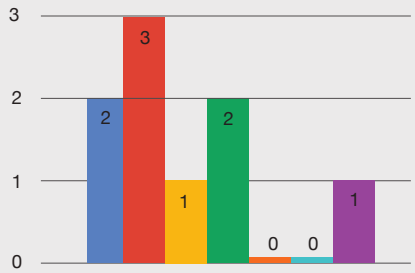


Fig 12. Industry's Response to Question 4



When it comes to whether local data storage will aid in the ease of access to data for law enforcement agencies, the three sectors are inclined to agreeing with the precedent. Only ~18% disagree, while another 18% agree to some extent.

12.3.5 Question 5: Is it Possible to develop a System of Voluntary Cross-border Transfer of data for India with other nations?

Fig 13. Civil Society's Response to Question 5

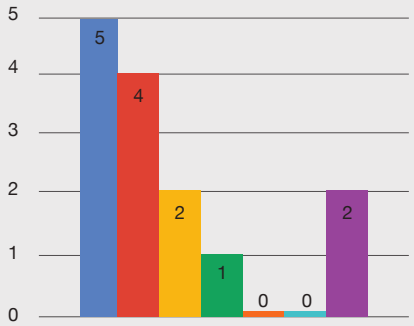


Fig 14. Academia's Response to Question 5

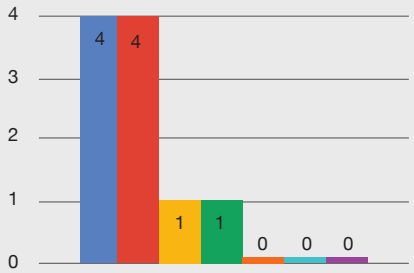
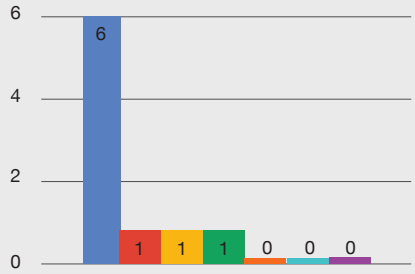


Fig 15. Industry's Response to Question 5



There is belief in the idea that it is theoretically possible to develop a system of voluntary cross-border data flows which enable the transfer of data. ~45% of the respondent base agrees with the idea while ~27% endorse it 'to some extent'.

12.3.6 Question 6: Will data localisation help in making Indian data more secure?

Fig 16. Civil Society's Response to Question 6

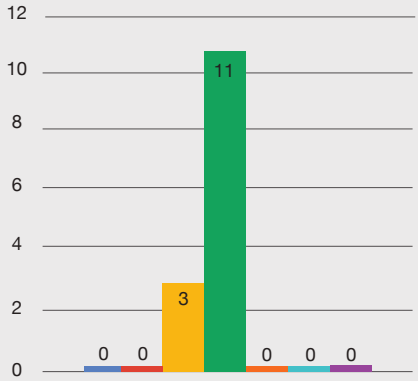


Fig 17. Academia's Response to Question 6

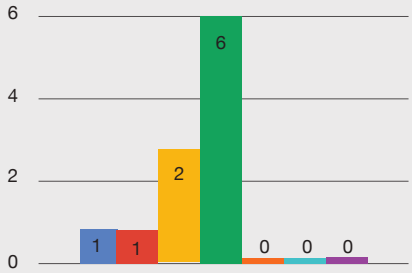
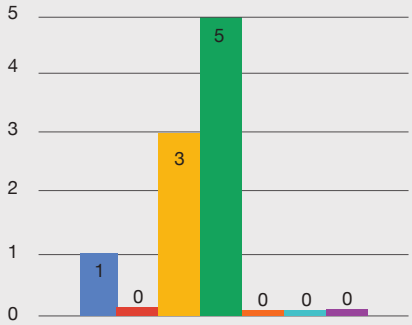


Fig 18. Industry's Response to Question 6



~66% of the total respondents claim that local storage of data will not help in making it more secure. This is in stark contrast to the 6% of the respondents believe that the location of data will have a positive impact on its security. ~24% of the base were unsure about the statement.

12.3.7. Question 7: Will local storage help in auditing of the data processed by fiduciaries in India?

Fig 19. Civil Society's Response to Question 7

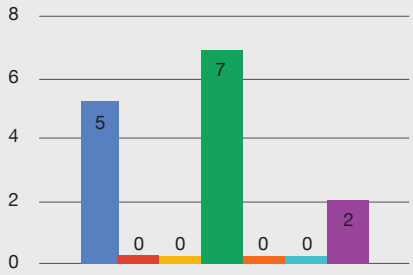


Fig 20. Academia's Response to Question 7

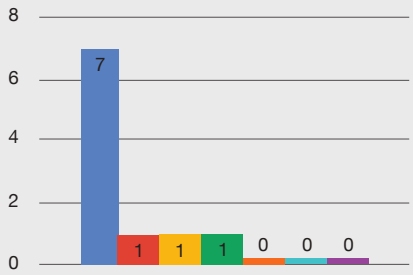
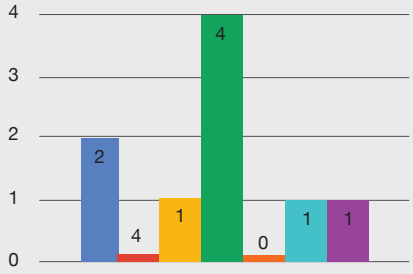


Fig 21. Industry's Response to Question 7



The respondents are split when it comes to whether local storage will help in the auditing of the data processed by fiduciaries in India. ~42% of the base agrees with the statement while ~36% of the respondents disagree. ~10% were non-answers as well.

12.2.8 Question 8: Is data localisation the only answer to create a Vibrant Digital Economy?

Fig 22. Civil Society's Response to Question 8

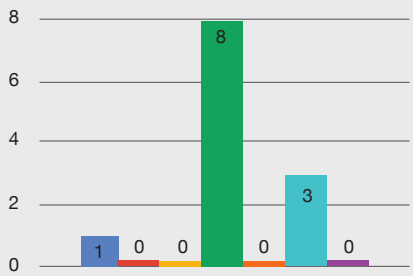


Fig 23. Academia's Response to Question 8

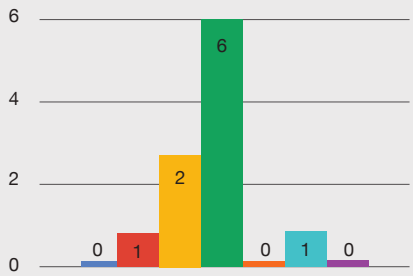
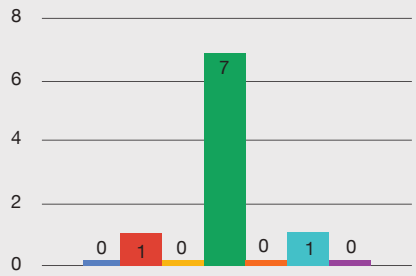


Fig 24. Industry's Response to Question 8



~66% of the total respondents claim that local storage of data will not help in making it more secure. This is in stark contrast to the 6% of the respondents believe that the location of data will have a positive impact on its security. ~24% of the base were unsure about the statement.

12.3.9 Question 9: Does local storage help in Improving Network Latencies?

Fig 25. Civil Society's Response to Question 9

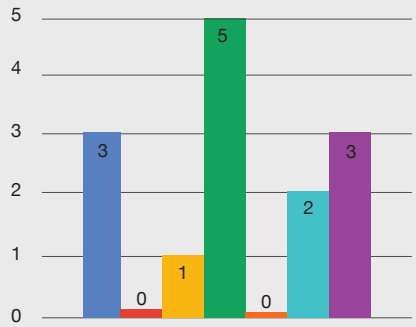


Fig 26. Academia's Response to Question 9

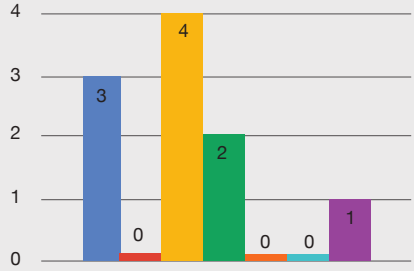
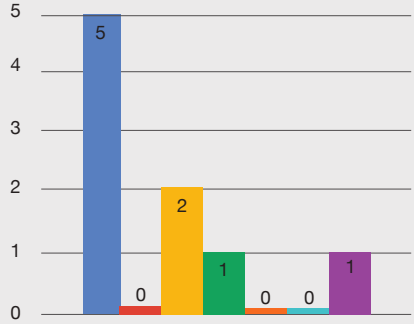


Fig 27. Industry's Response to Question 9



~33% of the people surveyed believed that local storage will help in improving network latencies. ~21% were unsure while ~25% did not think that localisation will have an effect on network latencies.

12.3.10 Question 10: Will local data storage give a Level Playing Field to Indian Technology Firms?

Fig 28. Civil Society's Response to Question 10

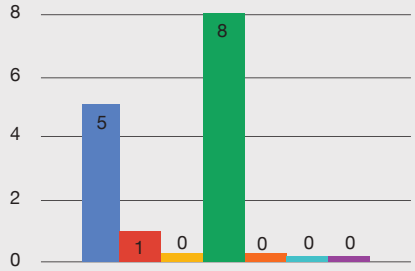


Fig 29. Academia's Response to Question 10

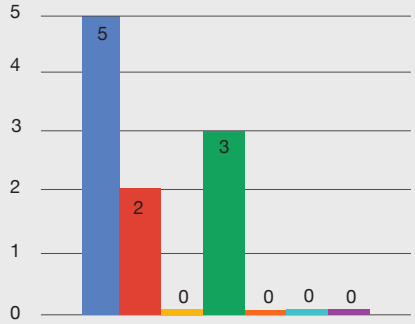
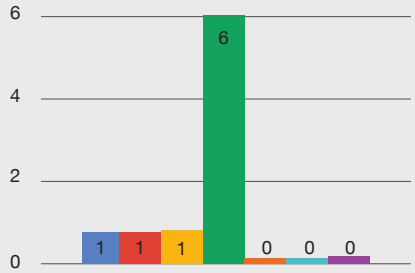


Fig 30. Industry's Response to Question 10



51% of the respondents believed that local data storage will not give a level playing field to Indian technology firms. ~33% of the base agreed with the precedent. However, only ~11% of industry approved of the same, compared to 50% of academia and ~36% of civil society.

12.3.11 Question 11: Is Data Transfer from Undersea Cables a Risk to Security?

Fig 31. Civil Society's Response to Question 11

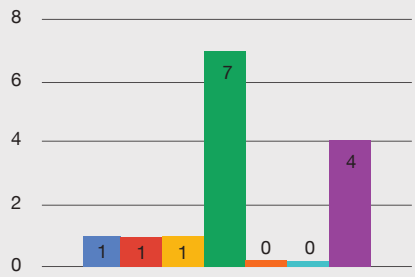


Fig 32. Academia's Response to Question 11

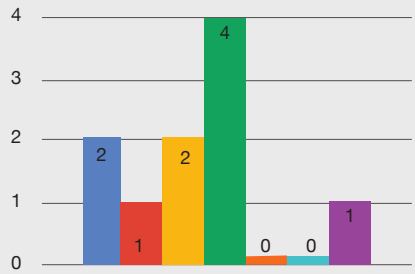
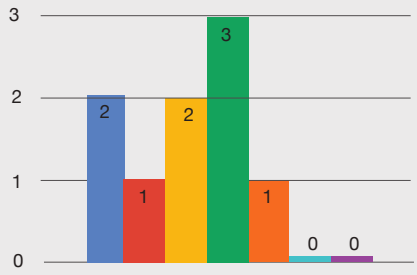


Fig 33. Industry's Response to Question 11



The respondents were sceptical on whether data transfer from undersea cables would be a risk to security. ~42% did not think that undersea cables were a security threat while ~15% believed in the contrary. ~15% were also unsure about the subject.

12.3.12 Question 12: Will local data storage and presence of data fiduciaries in India expand India's tax jurisdiction over the data processed by foreign fiduciaries?

Fig 34. Civil Society's Response to Question 12

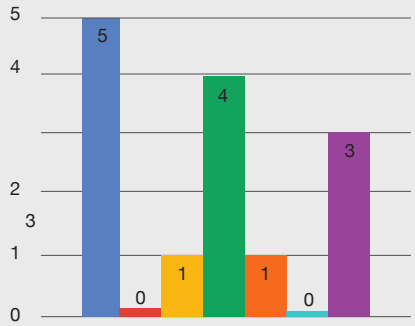


Fig 35. Academia's Response to Question 12

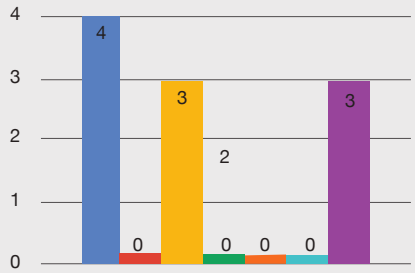
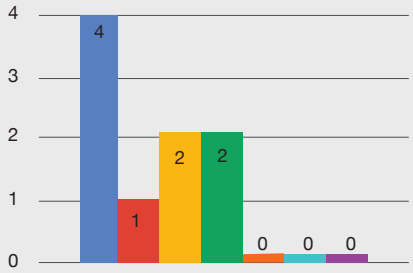


Fig 36. Industry's Response to Question 12



~40% of the respondents believe that local storage of data will expand India's tax jurisdiction over data processed by foreign fiduciaries. Another 18% provided non-answers, highlighting a lack of understanding in the area.

12.4 Thematic Analysis of Reports and Comments from Experts

12.4.1 Introduction

This section contains analysis in qualitative research. The thematic analysis pinpoints, examines, and records patterns(or themes) within the reports and comments by the experts in the field of government, academia, civil societies etc. The themes were also extracted from the stakeholder consultations conducted by The Dialogue in its roundtables, symposiums and conferences across various verticals covering topics such as data security, data protection, cross-border data flow, The Personal Data Protection Bill, 2018 etc. The identification and categorization of the themes were done through summarizing and highlighting key recommendations and concerns/challenges from the aforementioned consultations and reports by experts.

12.4.2 Methodology

The methodology is a critical component of this data localisation study that considers key qualitative analysis to study the impact of data localisation from a global perspective.

The description of the parameters are divided into the following columns:

1. Theme - containing themes abstracted from the research and consultations

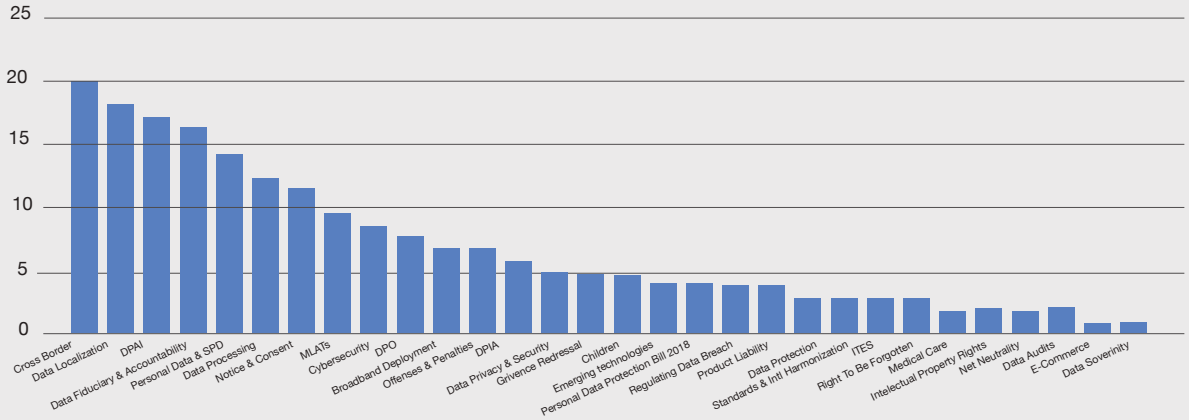
2. Count - The number of times a particular theme was mentioned

3. Summary - Contains key recommendations, insights and concerns/problems relating to each theme

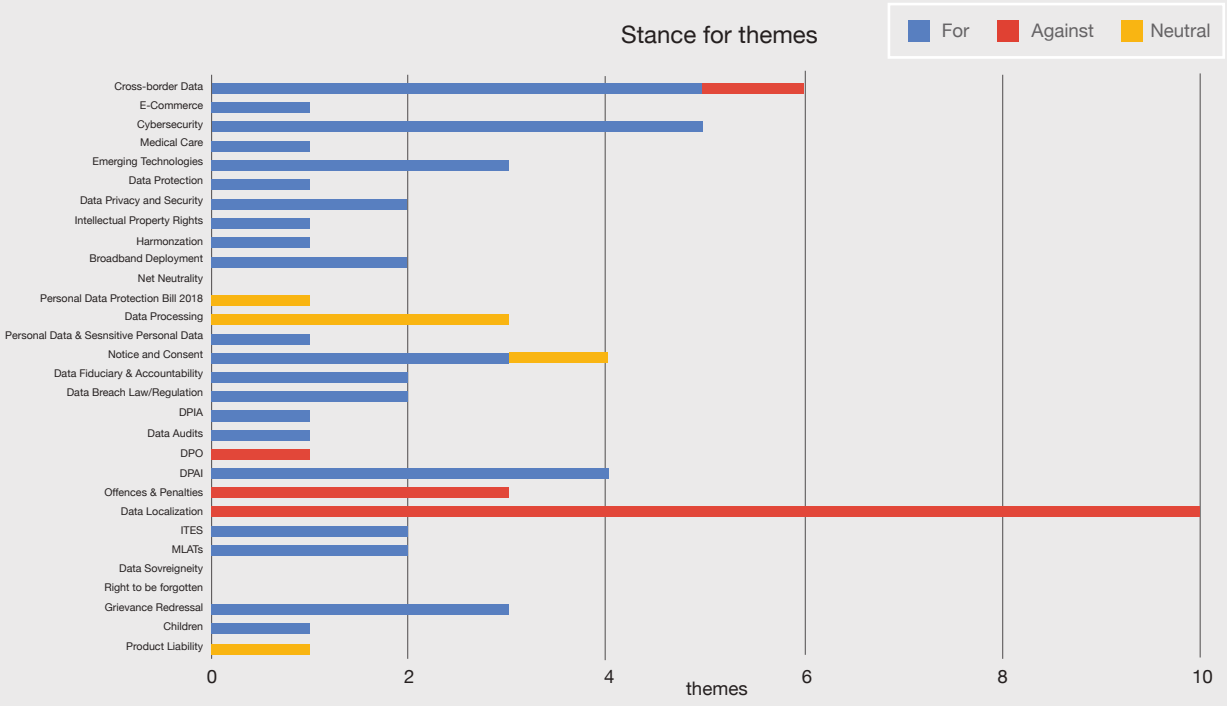
4. Stance - The stance taken by the stakeholders mapped on 1:1 basis; For, Against and Neutral

12.4.3 Findings

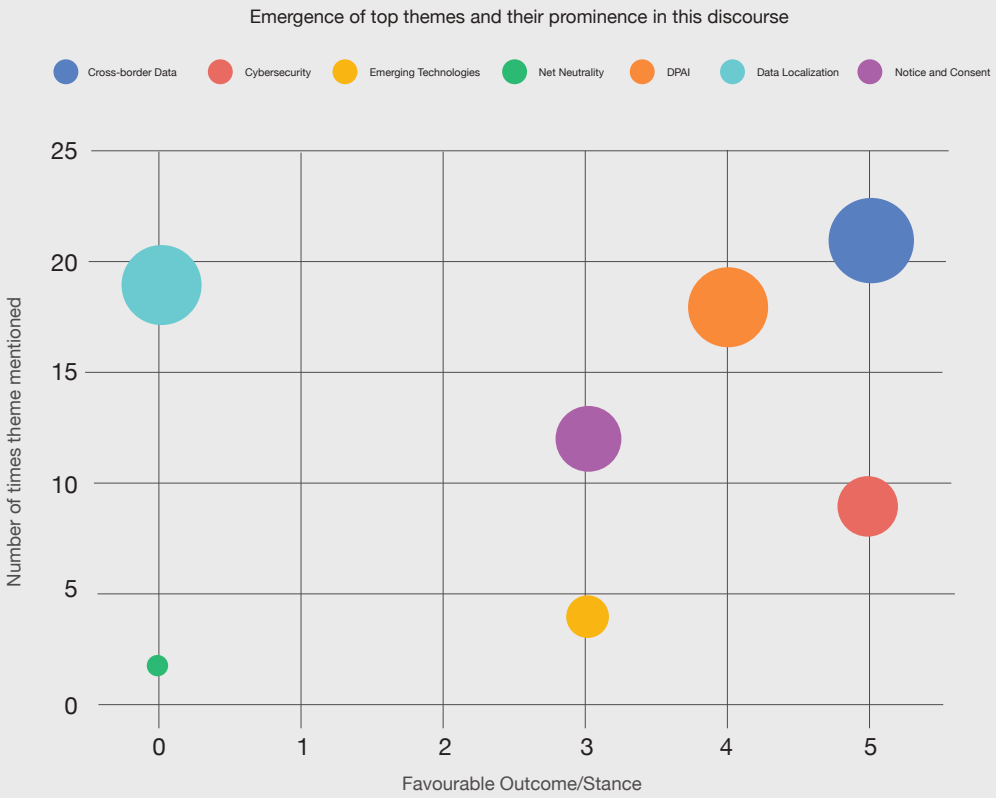
The findings clearly points to how important cross-border data flow and the impact of data localization is in the discourse of data protection in India. From the chart below, the top themes that emerges from our stakeholders are Cross-Border Data Flow and Promotion of
Trade, Data Localization, Roles and Responsibilities of DPIA, Data Fiduciaries and Accountability. It is also observed that other sub-topics in the sphere of this data localisation discourse such as MLATs, Broadband Deployment and Grievance Redressal forms a major chunk of the analysis.



The test of objectivity is done through observing what stances are taken by the stakeholders and experts across themes. The graph below reflects that stance (For, Against, Neutral). While Cross-Border Data Flow, Cybersecurity, Emerging Technologies show a clear of a positive (For) stance, themes like Data Localization and Offences & Penalties doesn't sit very well with the people involved in the discourse of data protection.



From our analysis, the top themes that emerged were Cross-Border Data Flow, Cybersecurity, Emerging Technologies, DPAI, Data Localization and Notice & Consent. An interesting insight that came out from the below bubble graph is the prominence of these themes.



As we plot the count of favourable (For stance) against the number of times a theme has been mentioned, we see a 2D vector space where the bubbles towards the top-right side depicting themes that have the highest mentions among the stakeholder consultations and report as well as having a For stance.

Data Localization emerges as one of the topic which has a higher count in the discourse but with a stance of Against.

Recommendations and Identifying Key Areas of Focus

Evaluating arguments presented in the chapters above, the report has a few key recommendations for storage and the future of India vis-a-vis transborder data flows.

1. Reforming the MLAT Process

To enable better law enforcement, it is essential to reform the MLATs by granting certainty to practices and procedures while minimizing discretion. Certain specific situations may be spelt out wherein the agencies have to act in a time-bound manner as long as the prescribed procedure for requesting information and access has been followed. The conditionality and procedural for the sharing of personal data by the host country to the agency of a foreign country needs to be mentioned without any ambiguities. The requirements, procedure and timelines for emergencies may be separately identified and prescribed. The Ministry of Home Affairs (MHA) should also build capacity and expertise to receive and review requests, establishing a dedicated team of legal officers trained in international criminal law and law enforcement agents on deputation. One way to achieve this is by digitizing the MLAT process, while simultaneously streamlining supplementary information and introducing internal timelines.

2. Enter into Global Privacy Frameworks and Data Sharing Agreements

India should look to enter into data sharing agreements with countries to ensure criminals are appropriately brought to justice while protecting an individual's right to privacy and promoting GDP growth.

The way forward would be to signing a data sharing agreement under the Cloud Act, 2018 with the US and also seeking to work with EU after qualifying the adequacy requirements. There are certain eligibility conditions given under the Act which include domestic privacy protection laws, substantive and procedural laws on cybercrime and electronic evidence, accountability and transparency mechanisms.

At the same time, India should focus at harmonising its domestic data protection standards with the APEC and ASEAN nations with an eye on interoperability with the APEC CBPR system developed by the forum.

Signing data sharing agreements with actors such as the US, EU, and ASEAN would also double as a strategic maneuver towards building better and more concrete relations with said actors.

3. Legal security of data stored in India a due-process of law for access to data

The following factors must be adhered to before data is accessed by the state for law enforcement and investigation purposes:

(i) An inclusive definition of the phrase 'Security of State.'

(ii) The entities/bodies which are authorised to process personal data. This list could be an inclusive list with the flexibility of updating the list.

(iii) An inclusive list of situations demanding processing of personal data.

(iv) A safety-net regulatory mechanism to approve processing of personal data (ring-fenced from political or economic influence).

(v) An oversight mechanism.

On security: The law for ensuring security for the data stored in India should address the issues from the following perspectives:

(i) Technical Measures – prescribing the standards and specifications that need to be complied by the data processors & data fiduciaries. There must be enabling provisions to prescribe the standards &specifications as they evolve.

(ii) Physical Measures – prescribing the physical conditions viz., location, situation, construction, layout, etc., of the centers where the data is to be processed.

(iii) Access Control – regulating the process and authority for access to and handling of the data being processed.

(iv) Disaster Management & Recovery – prescribing the specifications for recovering & damage control in the event of a breach.

4. Incentivising the Development of Data Centres

As discussed in chapter 10, India needs to address multiple areas when it comes to presenting itself as a viable destination to host data centres. There are challenges on the infrastructural and policy front.

Considering the former first, infrastructure in India needs to be developed to provide for the demands of data centres. Perhaps most importantly, there is the problem of electricity shortage.

Approximately a quarter of India's population does not have access to electricity. This is a major challenge when it comes to running a data center as an average 75% of the costs involved in running a data center are energy requirements. So not only is there a need for access to electricity, but a requirement to achieve the same while maintaining costs.

This is an objectively challenging hurdle and one which the government and private sector should collaborate to overcome. A possible way forward could be to encourage the private sector to power their own data centres. Passing this responsibility to the private sector will ensure maximum efficiency when it comes to minimising cost.

Similar measures would have to be taken to meet the cooling and internet demands of data centers. Encouraging private sector to take the lead in infrastructure building and facilitating for their own data centers would mean incentivising the same through a relaxation in duties and a streamlining of regulation to improve ease of doing business.

5. Adopting a Standards-based Approach to Sharing Data

Evaluating the rationale behind data localization helps us identify that a key reason for this push is the need to secure the data of Indian citizens.

That is an important goal and can be achieved through different measures. One of the more common approaches to this is setting security standards for data centers and allowing them to host data if said standards are met.

Adopting a standards approach, say, in case of personal financial data, would give the international community a better idea of the requirements India has when it comes to securing our data. It would allow us to dictate access requirements while ensuring adequate provision of infrastructure.

Conclusion

The importance of the ability to share data is as important as the existence of data itself. All things considered, the risks of data localization outweigh the benefits. Cross-border data flows are and will remain instrumental in shaping the future of the world. In an age where the digital economy and traditional economy are inextricable, India could bank on cross-border data flows to fuel its digital industry.

However, recent policy measures and recommendations suggest that following a rising global trend, India might adopt a different approach and move towards data localization. There are multiple reasons for why India is approaching data sharing the way it is. Ranging from rising strategic concerns from threats such as foreign surveillance, to economic aspects like domestic protectionism, data localization is viewed as a solution or at least part of it.

This study finds that this approach may backfire for a number of reasons. For instance, the location of data does not translate into access or ownership. In addition, localisation might save Indian data from foreign threats but placing the servers on home soil increases the risk of domestic threats while also dealing with the challenge of inadequate infrastructure.

A more comprehensive look at the pros and cons of data localization will reveal that there are better alternatives available to achieve the ends that localization might appear as a means to. Increased security and access is possible when servers are placed abroad while saving costs for all stakeholders involved. As far as the law enforcement lens is concerned, the problem lies not with localisation but with MLATs. Taking steps to tackle the speed and efficiency of the MLAT process will be a stable solution for the long-term.

India needs to back the IT industry to fuel economic growth, and localization will have the opposite effect. Forcing localization will not create the conditions, infrastructural, economic, or technical, for the setup of multiple data centres. Instead, incentivising these efforts will have a more positive effect.

So anything localization can do, other measures can do better. More importantly, they may be able to do it without limiting opportunities for future progress. The costs of data localisation outweigh the benefits. At a time where India much choose between free cross-border data flows or data localization, it would be in her best interests to go with the former.

Bibliography

"20 years of Internet in India: On August 15, 1995 public Internet access ...." 15 Aug. 1995, https://www.news18.com/news/tech/20-years-of-internet-in-india-on-august-15-1995-public-internet-access-was-launched-in-india-1039859.html. Accessed 1 Nov. 2018.

"5 factors driving the growth of data analytics in India - YourStory." 16 Dec. 2016, https://yourstory.com/2016/12/growth-data-analytics-india/. Accessed 2 Nov. 2018.

"12 Best Zoho Products: Reviews Of The Most Popular Services ...." 9 Nov. 2018, https://financesonline.com/top-zoho-products-reviews-popular-services/. Accessed on 14 Nov. 2018.

"2018 The Economics of Data Flows in Asia Pacific." http://www.asiacloudcomputing.org/research/2018-research/2018-the-economics-of-data-flows-in-asia-pacific. Accessed 16 Nov. 2018.

“2016 Conducive Policy and Regulatory Environment to incentivise data center infrastructure.” https://cms.iamai.in/Content/PolicyPapers/7065f212-0eb7-4a05-a1aa-3bc9433eb75f.pdf Accessed 24 Oct. 2018

"18 U.S. Code § 2523 - Executive agreements on access to data by ...." https://www.law.cornell.edu/uscode/text/18/2523. Accessed on 15 Nov. 2018.

"A Data Localization Free-for-All? | Center for Strategic and ...." 9 Mar. 2018, https://www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/data-localization-free-all. Accessed 26 Oct. 2018.

"About APEC - Asia-Pacific Economic Cooperation." https://www.apec.org/About-Us/About-APEC. Accessed on 15 Nov. 2018.

"About Data Centers - TIA-942.org." http://www.tia-942.org/content/162/289/About_Data_Centers. Accessed on 14 Nov. 2018.

"About Us - GSMA." https://www.gsma.com/aboutus/. Accessed 26 Oct. 2018.

"Access to Electronic Data by Third-Country Law Enforcement ...." https://www.researchgate.net/publication/289539859_Access_to_Electronic_Data_by_Third-Country_Law_Enforcement_Authorities_Challenges_to_EU_Rule_of_Law_and_Fundamental_Rights. Accessed 2 Nov. 2018.

"Addressing the Impact of Data Location Regulation in Financial Services." 22 May. 2015, https://www.cigionline.org/publications/addressing-impact-data-location-regulation-financial-services. Accessed 26 Oct. 2018.

"Amazon opens data centers in India - The Hindu Business Line." 28 Jun. 2016, https://www.thehindubusinessline.com/info-tech/amazon-opens-data-centers-in-india/article8783403.ece. Accessed 26 Oct. 2018.

"Analytics & Data Science Industry In India: Study 2018." 18 Jun. 2018, https://www.analyticsindiamag.com/analytics-data-science-industry-in-india-study-2018-by-analytixlabs-aim/. Accessed on 14 Nov. 2018.

"Apple opposes order to hack gunman's phone - CNN - CNN.com." 18 Feb. 2016, https://www.cnn.com/2016/02/16/us/san-bernardino-shooter-phone-apple/index.html. Accessed 31 Oct. 2018.

"Articles & Publications AUGUST 2018 - Induslaw." 3 Aug. 2018, https://induslaw.com/app/webroot/publications/pdf/alerts-2018/Personal_Data_Protection_Bill_2018.pdf. Accessed on 15 Nov. 2018.

"Artificial Intelligence Could Add $957 Billion to Indian Economy ...." 21 Dec. 2017, https://newsroom.accenture.com/news/artificial-intelligence-could-add-957-billion-to-indian-economy-according-to-new-research-by-accenture.htm . Accessed 31 Oct. 2018.

"Bengaluru: what's next for India's tech capital? | Business to business ...." 3 Jul. 2018, https://www.theguardian.com/business-to-business/2018/jul/03/bengaluru-whats-next-for-indias-tech-capital. Accessed 1 Nov. 2018.

"Best Practices for Data Centers: Lessons Learned from ... - CiteSeerX." http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=AB9AA88224E428BCB86D9EEB836F41D8?doi=10.1.1.207.3280&rep=rep1&type=pdf . Accessed on 15 Nov 2018.

"Big Data, for better or worse: 90% of world's data ... - ScienceDaily." 22 May. 2013, https://www.sciencedaily.com/releases/2013/05/130522085217.htm. Accessed 26 Oct. 2018.

"Big data analytics to reach $16 billion industry by 2025: Nasscom, IT ...." 23 Jun. 2016, https://cio.economictimes.indiatimes.com/news/big-data/big-data-analytics-to-reach-16-billion-industry-by-2025-nasscom/52885901. Accessed 31 Oct. 2018.

“Big Data Analytics: What it is and why it matters I SAS” https://www.sas.com/en_us/insights/analytics/big-data-analytics.html. Accessed on 15 Nov 2018.

"BIF Recommendations for NTP on New Technologies - Broadband India ...." https://www.broadbandindiaforum.com/images/national-telecom-policy-2018/BIF-Recommendations-on-New-Technologies.docx. Accessed 5 Nov. 2018

"Black Money and Politics in India | Economic and Political Weekly - Epw." https://www.epw.in/journal/2017/7/special-articles/black-money-and-politics-india.html. Accessed 30 Oct. 2018.

"Brazil Legislators Bear Down on Internet Bill - Wall Street Journal." 13 Nov. 2013, https://www.wsj.com/articles/brazil-legislators-bear-down-on-internet-bill-1384384450. Accessed on 14 Nov. 2018

"Brazil's New Data Protection Law: The LGPD - Mondaq." 19 Sep. 2018, http://www.mondaq.com/brazil/x/737694/data+protection/Brazils+New+Data+Protection+Law+The+LGPD. Accessed on 15 Nov. 2018.

"Build Or Buy? The Economics Of Data Center Facilities - Data Centers." https://www.io.com/wp-content/uploads/2014/10/WhitePaper_Forrester_Build-or-Buy_Economics-of-Data-Center-Facilities.pdf. Accessed on 14 Nov.2018.

"Business Roundtable." https://www.businessroundtable.org/. Accessed 26 Oct. 2018.

Central Bureau of Investigation – India, MLATs, http://cbi.nic.in/interpol/mlats.php

"Chinese Data Localization Law: Comprehensive but Ambiguous - The ...." 7 Feb. 2018, https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/. Accessed 26 Oct. 2018.

"Consolidated FDI Policy Circular of 2017 | Department of Industrial ...." 28 Aug. 2017, http://dipp.nic.in/whats-new/consolidated-fdi-policy-circular-2017. Accessed on 15 Nov. 2018.

"Cross-Border Data Flows, Digital Innovation, and Economic Growth ...." http://www3.weforum.org/docs/GITR2016/WEF_GITR_Chapter1.2_2016.pdf. Accessed 26 Oct. 2018.

"Cross-Border Data Flows: Where Are the Barriers, and What Do They ...." 1 May. 2017, https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost. Accessed 13 Nov. 2018.

"Cross-Border Data Sharing Under the CLOUD Act - Federation Of ...." 23 Apr. 2018, https://fas.org/sgp/crs/misc/R45173.pdf. Accessed 2 Nov. 2018.

“Cross-Border Data Flows-Realising benefits and removing barriers” https://www.gsma.com/publicpolicy/cross-border-data-flows-realising-benefits-and-removing-barriers. Accessed on 15 Nov 2018.

"Data Is the New Oil of the Digital Economy | WIRED." https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/. Accessed 26 Oct. 2018.

"data nationalism - Emory Law." 19 Feb. 2015, http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf. Accessed 11 Nov. 2018

"Data Processing and Security Terms | Google Cloud Platform Terms ...." 7 Feb. 2017, https://-cloud.google.com/terms/data-processing-terms-20170207. Accessed 30 Oct. 2018.

"Data protection in Brazil: overview | Practical Law - Westlaw." https://content.next.westlaw.com/Document/I02064fc61cb611e38578f7ccc38dcbee/View/FullText.html?contextData=(sc.Default)&transitionType=Default. Accessed on 15 nov. 2018.

"Data localisation in India: Questioning the means and ends - NIPFP." 31 Oct. 2018, https://www.nipfp.org.in/media/medialibrary/2018/10/WP_2018_242.pdf. Accessed on 15 Nov. 2018.

"Data localisation norms could negatively impact India's GDP | analysis ...." 20 Jul. 2018, https://www.hindustantimes.com/analysis/data-localisation-norms-could-negatively-impact-india-s-gdp/story-A8HNFTjIDBM550HJiKbpnO.html. Accessed 1 Nov. 2018.

"Data Localization | Digital Import Export Trade | American Express FX ...." https://www.americanexpress.com/us/content/foreign-exchange/articles/data-localization-affects-digital-import-export-trade/. Accessed on 15 Nov. 2018.

""Data Minefield? How AI is Prodding Governments to Rethink Trade in ...." 3 Apr. 2018, https://www.bsa.org/news-and-events/bsa-in-the-news/2018/april/en-04032018-data-minefield-how-ai-is-prodding-governments-to-rethink-trade-in-data/?sc_lang=en. Accessed on 15 Nov. 2018.

"Department of Defense Accomplishments | Belfer Center for Science ...." https://www.belfercenter.org/publication/department-defense-accomplishments. Accessed 7 Nov. 2018.

"Digital globalization: the new era of global flows - McKinsey & Company." https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx. Accessed 26 Oct. 2018.

"Digital globalization: The new era of global ...." https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows. Accessed 26 Oct. 2018.

"Digital Information Security in Healthcare Act on Cards." 28 Aug. 2018, http://innohealthmagazine.com/newscope/digital-information-security-healthcare-act/. Accessed 10 Nov. 2018.

"Digital Security Risk Management for Economic and ... - OECD.org." 17 Sep. 2015, https://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf. Accessed 30 Oct. 2018.

"Do data center tax breaks help? - DCD." 27 May. 2015, https://www.datacenterdynamics.com/opinions/do-data-center-tax-breaks-help/. Accessed 2 Nov. 2018.

"Doing Business in Vietnam - PwC."
https://www.pwc.de/de/internationale-maerkte/assets/doing-business-in-vietnam.pdf. Accessed on 15 Nov. 2018.

"Draft Decree to implement Cybersecurity Law doesn't dampen ...."
https://www.lexology.com/library/detail.aspx?g=0d3f8017-8849-45db-b5d0-6947b790755f. Accessed on 15 Nov. 2018.

"Draft National E-commerce Policy: data localization and priority to ...." 7 Aug. 2018, https://www.medianama.com/2018/08/223-draft-national-e-commerce-policy-data-localization-and-priority-to-domestic-companies/. Accessed 26 Oct. 2018.

"E-commerce & the OECD Definition of Permanent Establishment - PE." 22 Dec. 2000, http://www.inter-lawyer.com/lex-e-scripta/articles/e-commerce-pe.htm. Accessed 13 Nov. 2018.

"E-commerce in India: Industry Overview, Market Size & Growth| IBEF." https://www.ibef.org/industry/ecommerce.aspx. Accessed 26 Oct. 2018.

"Edward Snowden: Leaks that exposed US spy programme - BBC News." 17 Jan. 2014, https://www.bbc.com/news/world-us-canada-23123964. Accessed 30 Oct. 2018.

"Electronic Commerce in India: Draft National Policy ... - MediaNama." https://www.medianama.com/wp-content/uploads/Draft-National-E-commerce-Policy.pdf. Accessed 26 Oct. 2018.

"EU-India relations, fact sheet - European External Action Service." https://eeas.europa.eu/delegations/india/4010/eu-india-relations-fact-sheet_en. Accessed 2 Nov. 2018.

"EUROPEAN COMMISSION Brussels, 10.1.2017 COM(2017) 8 final ...." 10 Jan. 2017, https://ec.europa.eu/newsroom/document.cfm?doc_id=41158. Accessed on 15 Nov. 2018

"Ex. Rept. 107-15 - MUTUAL LEGAL ASSISTANCE TREATIES WITH ...."
https://www.congress.gov/congressional-report/107th-congress/executive-report/15. Accessed on 15 Nov.2018.

"FAQs - MLAT."
https://www.mlat.info/faq. Accessed on 15 Nov. 2018

"framework on personal data protection - asean."
http://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf.Accessed on 15 Nov.2018.

"Federal Law No. 242-FZ. | wilmap." 14 May. 2018, https://wilmap.law.stanford.edu/en-

tries/federal-law-no-242-fz. Accessed 26 Oct. 2018.

"Glossary - Asia-Pacific Economic Cooperation." https://www.apec.org/Glossary. Accessed 2 Nov. 2018.

"Global Working Papers - Brookings Institution."https://www.brookings.edu/series/global-working-papers/ . Accessed on 15 Nov 2018.

"Government of India - DoT." http://www.dot.gov.in/sites/default/files/Amendment_UASL_1-2-06_1.pdf. Accessed on 15 Nov. 2018.

"Guidelines for Government Departments on - MeitY." 31 Mar. 2017, http://meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf. Accessed on 15Nov. 2018.

"Group of Governmental Experts on Developments in the Field of ...." 9 Apr. 2017, http://digitallibrary.un.org/record/799853?ln=en.Accessed on 15 Nov. 2018.

"GSMA: Free Flow of Data Across Borders Essential for Asia's Digital ...." 5 Sep. 2018, https://www.gsma.com/newsroom/press-release/gsma-free-flow-of-data-across-borders-essential-for-asias-digital-economies/.Accessed on 15 Nov. 2018.

"Hitting Refresh - Observer Research Foundation." 8 Aug. 2017, https://www.orfonline.org/wp-content/uploads/2017/08/ORF_SpecialReport_39_DataSharing.pdf. Accessed on 15 Nov. 2018.

"how artificial - Accenture." 30 Jun. 2017, https://www.accenture.com/t20170629T190038Z__w__/cn-en/_acnmedia/PDF-55/Accenture-How-Artificial-Intelligence-Can-Drive-Chinas-Growth.pdf. Accessed 31 Oct. 2018.

"How Much Data Do We Create Every Day? The Mind-Blowing Stats ...." 21 May. 2018, https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/. Accessed 26 Oct. 2018.

https://www.analyticsindiamag.com/analytics-data-science-industry-in-india-study-2018-by-analytixlabs-aim/

https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=CELEX:02016R0679-20160504&qid=1532348683434

https://www.oaic.gov.au/privacy-law/privacy-act/

https://www.oaic.gov.au/privacy-law/privacy-act/privacy-regulations

https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

Imarticus Learning and NASSCOM (2017) Analytics Employment Landscape in India, https://imarticus.org/wp-content/uploads/2017/04/Industry-Report-Analytics-%202017.pdf. Accessed on 14 Nov. 2018.

"Impact of e-commerce on SMEs in India - KPMG." https://assets.kpmg.com/content/dam/kpmg/pdf/2015/10/Snapdeal-Report_-Impact-of-e-Commerce-on-Indian-SMEs.pdf. Accessed 5 Nov. 2018.

"Impact of Taxes & Incentives on Data Center Locations - DocPlayer.net." https://docplayer.net/5244400-Impact-of-taxes-incentives-on-data-center-locations.html. Accessed on 14 Nov. 2018.

"In Our Wi-Fi World, the Internet Still Depends on Undersea Cables." 3 Nov. 2015, http://www.govtech.com/network/In-Our-Wi-Fi-World-the-Internet-Still-Depends-on-Undersea-Cables.html. Accessed 5 Nov. 2018.

"India's data centre market to reach $4.5 billion by 2018: IAMAI ...." 26 May. 2016, https://telecom.economictimes.indiatimes.com/news/indias-data-centre-market-to-reach-4-5-billion-by-2018-iamai/52443770. Accessed on 14 Nov. 2018.

"India: Information Technology (Reasonable Security Practices and ...." 4 Sep. 2017, https://www.lexology.com/library/detail.aspx?g=35f56a2a-c77c-49e7-9b10-1ce085d981dd. Accessed on 15 Nov. 2018.

"India mobile phone users 2013-2019 - Statista." https://www.statista.com/statistics/274658/-forecast-of-mobile-phone-users-in-india/. Accessed 1 Nov. 2018.

"India Should Let Data Roam Free - Bloomberg." 13 Sep. 2018, https://www.bloomberg.com/view/articles/2018-09-13/india-should-allow-consumer-data-to-flow-offshore . Accessed 26 Oct. 2018.

"India's 'worst water crisis in its history' is only going to get worse ...." 17 Jun. 2018, https://www.independent.co.uk/news/world/asia/india-water-crisis-shortage-niti-aayog-report-drought-mismanagement-a8403286.html. Accessed on 14 Nov. 2018.

"Indian IT-BPM industry GDP share 2009-2017 | Statistic." https://www.statista.com/statistics/320776/contribution-of-indian-it-industry-to-india-s-gdp/. Accessed 31 Oct. 2018.

"Indians on an average consume 1GB data a day on smartphones ...." 27 Sep. 2018, https://www.indiatvnews.com/technology/news-indians-on-an-average-consume-1gb-data-a-day-on-smartphones-466020. Accessed 31 Oct. 2018.

"India Economy Indian Economy, business opportunities in India ...." https://www.globaltenders.com/economy-of-india.php/. Accessed on 14 Nov. 2018.

"Indonesia Telecoms and Media – Getting The Deal Through – GTDT." https://gettingthedealthrough.com/area/39/jurisdiction/42/telecoms-media-indonesia/. Accessed on 14 Nov. 2018.

"Industry Study 2018_Final_18 June - Analytics India Magazine." https://www.analyticsindiamag.com/analytics-data-science-in-dustry-in-india-study-2018-by-analytixlabs-aim/?aid=25498&sa=0. Accessed on 14 Nov. 2018.

"International data-sharing norms: from the OECD to the General Data ...." 1 Aug. 2018, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6132662/. Accessed 2 Nov. 2018.

"Internet of Things Will Deliver $ 1.9 Trillion Boost to Supply Chain and ...." 16 Apr. 2015, https://www.businesswire.com/news/home/20150416006351/en/In-ternet-Things-Deliver-1.9-Trillion-Boost-Supply. Accessed 26 Oct. 2018.

"Internet matters - McKinsey & Company." https://www.mckinsey.com/~/media/McKinsey/In-dus-tries/High%20Tech/Our%20Insights/Internet%20matters/MGI_internet_matters_exec_summary.ashx. Accessed 26 Oct. 2018.

"Internet usage in India - Statista." https://www.statista.com/topics/2157/internet-usage-in-india/. Accessed on 14 nov. 2018.

"Internet users in India expected to reach 500 million by June: IAMAI." 20 Feb. 2018, https://economictimes.indiatimes.com/tech/internet/inter-net-users-in-india-expected-to-reach-500-million-by-june-iamai/articleshow/63000198.cms. Accessed 1 Nov. 2018.

"IT export growth to be lower in 2017-18 at 7-8pc: Nasscom - YourStory." 23 Jun. 2017, https://yourstory.com/2017/06/it-export-growth-lower-nasscom/. Accessed 31 Oct. 2018.

“Japan, EU Launching High-Level Talks on Safe Data Transfers,” Nikkei Asian Review, accessed October 21, 2018.

"July 25, 2016 Shri A. Robert J. Ravi Advisor - Telecom Regulatory ...." 25 Jul. 2016, https://t-rai.gov.in/sites/default/files/201609070951396640421ITI_0.pdf. Accessed 26 Oct. 2018.

"Key Highlights From Srikrishna Committee Report on Data ... - The Quint." 27 Jul. 2018, https://www.thequint.com/news/india/key-highlights-from-sri-krishna-committee-report-on-data-protection. Accessed 26 Oct. 2018.

"LINE, WeChat, WhatsApp, Facebook: Where Most Of Asia's Business ...." 8 May. 2017,

https://www.forbes.com/sites/vinnielauria/2017/05/08/line-we-chat-whatsapp-facebook-where-most-of-asias-business-deals-are-being-done/. Accessed 2 Nov. 2018.

"Living in the Dark: 240 Million Indians Have No Electricity - Bloomberg." 24 Jan. 2017, https://www.bloomberg.com/news/features/2017-01-24/living-in-the-dark-240-million-indians-have-no-electricity. Accessed on 14 Nov. 2018.

"Localization Barriers to Trade: Threat to the Global Innovation ... - ITIF." 1 Sep. 2013, http://www2.itif.org/2013-localization-barriers-to-trade.pdf. Accessed 1 Nov. 2018.

"Managing Alternatives for Privacy, Property and INternet Governance ...." https://cordis.europa.eu/project/rcn/111214_en.html. Accessed on 15 Nov.2018.

Market Equations (2017) About Market Equations, http://www.marketequations.com/about-us.html. Accessed on 14 Nov. 2018.

"MLATs - Observer Research Foundation." 8 Aug. 2017, https://www.orfonline.org/wp-content/uploads/2017/08/MLAT-Book.pdf.Accessed on 15 Nov. 2018.

"Microsoft nabs Indian e-commerce giant Flipkart for Azure as cloud ...." 20 Feb. 2017, https://venturebeat.com/2017/02/20/indian-internet-giant-flipkart-partners-with-microsoft/. Accessed on 14 Nov. 2018.

"Most powerful engine of India's growth: Service MSMEs - The ...." 27 Jan. 2018, https://economictimes.indiatimes.com/small-biz/sme-sector/-most-powerful-engine-of-indias-growth-service-msmes/articleshow/62670137.cms. Accessed 5 Nov. 2018.

"mutual legal assistance - US Department of State." https://www.state.gov/documents/organization/111634.pdf. Accessed on 15 Nov. 2018.

"Mutual Legal Assistance Treaties (MLATs) - Carnegie Mellon ...." 14 May. 2015, https://www.heinz.cmu.edu/~acquisti/SHB2015/Swire.docx. Accessed on 15 Nov. 2018.

"mutual legal assistance requests - The Ministry of External Affairs." http://mea.gov.in/Images/pdf1/MUTUAL_LEGAL_ASSISTANCE_REQUESTS.pdf. Accessed on 15 Nov. 2018.

"Nasscom: Indian IT to clock 7-9% growth in FY19, job creation to ...." 20 Feb. 2018, https://economictimes.indiatimes.com/tech/ites/indian-software-services-sector-to-grow-7-9-in-fy19-nasscom/articleshow/62995685.cms. Accessed 26 Oct. 2018.

"New Telecom Policy 1999 (India) - unpan1.un.org, 24.07.2012." http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan040889.pdf. Accessed on 14 Nov. 2018.

"New Themes in Innovation Policy – New ... - INNOGRIPS Logo." http://innogrips.empirica.biz/-fileadmin/innogrips/documents/01_policy%20briefs/ig_policybrief_6_new-themes.pdf. Accessed 26 Oct. 2018.

"Notifications - Reserve Bank of India." 6 Apr. 2018, https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0. Accessed on 15 Nov. 2018.

"Number of Indian internet users will reach 500 million ... - Times of India." 20 Feb. 2018, https://timesofindia.indiatimes.com/business/india-business/-number-indian-internet-users-will-reach-500-million-by-june-2018-iamai-says/articleshow/62998642.cms. Accessed 5 Nov. 2018.

"Outsourcing to India | Whitepaper - Back Office Pro." https://www.backoffice-pro.com/white-paper/outsourcing-to-india/. Accessed 26 Oct. 2018.

"PM Modi Defends His Decision Of Demonetisation, Says It Has Led To ...." 5 Oct. 2017, https://www.indiatimes.com/news/india/pm-modi-defends-his-decision-of-demonetisation-says-it-has-led-to-cashless-economy-331086.html. Accessed 1 Nov. 2018.

"Press Release: ITU releases 2016 ICT figures ...." 22 Jul. 2016, https://www.itu.int/en/media-center/Pages/2016-PR30.aspx. Accessed 26 Oct. 2018.

"Privacy and the Cloud: Issues in Cloud Law - Australia - HG.org." https://www.hg.org/legal-articles/privacy-and-the-cloud-issues-in-cloud-law-australia-26496. Accessed 2 Nov. 2018.

"Promoting stability in ASEAN's cyberspace | Clingendael spectator." 23 Aug. 2018, https://spectator.clingendael.org/en/publication/promoting-stability-aseans-cyberspace. Accessed 2 Nov. 2018.

"Public Cloud Powers Business Transformation at Healthcare Major ...." https://enterprise.microsoft.com/en-in/customer-story/industries/health/public-cloud-powers-business-transformation-healthcare-major/. Accessed 26 Oct. 2018.

"Regional Privacy Frameworks and Cross-Border Data Flows - GSMA." https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf. Accessed 26 Oct. 2018

"Renewable energy country attractiveness index (RECAI) 43 - EY." https://www.ey.com/Publication/vwLUAssets/EY-renewable-energy-country-attractiveness-index-recai-43/$FILE/EY-renewable-energy-country-attractiveness-index-recai-43.pdf. Accessed 2 Nov. 2018.

"Reserve Bank of India - Notifications." 6 Apr. 2018, https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0. Accessed 30 Oct. 2018.

"Revealed: Facebook hate speech exploded in Myanmar during ...." 3 Apr. 2018, https://www.theguardian.com/world/2018/apr/03/revealed-facebook-hate-speech-exploded-in-myanmar-during-rohingya-crisis. Accessed 31 Oct. 2018.

"Regional Privacy Frameworks and Cross-Border Data Flows - GSMA." https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Exec-Summary_Sept-2018.pdf. Accessed on 15 Nov. 2018.

"Regulating for a digital economy: Understanding the importance of ...." 20 Mar. 2018, https://www.brookings.edu/research/regulating-for-a-digital-economy-understanding-the-importance-of-cross-border-data-flows-in-asia/ . Accessed on 15 Nov 2018.

"Russia Data Localization Requirement at a Glance - Bryan Cave Data ...." http://bryancavedatamatters.com/wp-content/uploads/2015/05/Russia-Data-Localization-Requirement-at-a-Glance.pdf. Accessed on 15 Nov. 2018.

"Should You Choose a Cloud or On-Premise E-commerce Platform?." http://www.netsuite.com/portal/resource/articles/ecommerce/should-you-choose-cloud-on-premise-ecommerce-platform.shtml. Accessed on 14 Nov. 2018.

"Singapore Joins APEC Data Privacy System - Asia-Pacific Economic ...." 7 Mar. 2018, https://www.apec.org/Press/News-Releases/2018/0307_CBPR.Accessed on 15 Nov.2018.

"SME Sector in India – Statistics, Trends, Reports – EVOMA." https://evoma.com/business-centre/sme-sector-in-india-statistics-trends-reports/. Accessed on 15 Nov. 2018.

"Strong Winds Ahead for Cloud Computing: Can Data Localization ...." 29 Apr. 2016, https://www.rand.org/blog/2016/04/strong-winds-ahead-for-cloud-computing-can-data-localization.html. Accessed 5 Nov. 2018.

"Susan Ariel Aaronson | Centre for International Governance Innovation." https://www.cigionline.org/person/susan-ariel-aaronson. Accessed on 15 Nov.2018.

"Text - H.R.4943 - 115th Congress (2017-2018): CLOUD Act ...." 6 Feb. 2018, https://www.-congress.gov/bill/115th-congress/house-bill/4943/text. Accessed 2 Nov. 2018.

"The APEC Cross-Border Privacy Rules—Now That We've Built It, Will ...." https://iapp.org/news/a/the-apec-cross-border-privacy-rules-now-that-weve-built-it-will-they-come/. Accessed 2 Nov. 2018.

"The costs of data localisation: friendly fire on economic recovery - ECIPE." http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf. Accessed 13 Nov. 2018.

"The Debate – Data Localization And Its Efficacy - Data Protection - India." 17 Sep. 2018, http://www.mondaq.com/india/x/736934/Data+Protection+Privacy/The+Debate+Data+Localization+And+Its+Efficacy. Accessed 26 Oct. 2018.

"the drafting of a Legal Instrument on Government-led Surveillance and ...." 10 Jan. 2018, http://www.ohchr.org/Documents/Issues/Privacy/DraftLegalInstrumentGovernmentLed.pdf. Accessed on 15 Nov.2018.

“The e-Commerce Policy Draft: A Sweet & Sour Mix” by Lex Witness Bureau; Vol. 10 Issue 2; September 2018

"The Emerging Trend of Data Localization – Columbia Science and ...." 1 Mar. 2018, http://stlr.org/2018/03/01/the-emerging-trend-of-data-localization/. Accessed 1 Nov. 2018.

"The Flow Of Data Across Borders - USCIB." https://www.uscib.org/uscib-content/uploads/2016/03/2016_03_The-Flow-of-Data-Across-Borders_A-BIAC-Trade-Committee-Policy-Pe....pdf. Accessed 31 Oct. 2018.

"The GDPR - European Commission - Europa EU." https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf. Accessed on 15 Nov. 2018.

"The Great Indian Big Data Talent Gap - Great Learning." 10 Apr. 2017, https://www.greatlearning.in/blog/the-great-indian-big-data-talent-gap/. Accessed on 14 Nov. 2018.

"The Global Information Technology Report 2016." https://www.wsj.com/public/resources/documents/GITR2016.pdf. Accessed 26 Oct. 2018.

“The Global Risk Report 2017 12th Edition - World Economic Forum” http://www3.weforum.org/docs/GRR17_Report_web.pdf. Accessed on 15 Nov 2018.

"The Harms of Forced Data Localization — Leviathan Security." 25 Feb. 2015, https://www.leviathansecurity.com/blog/the-harms-of-forced-data-localization. Accessed 31 Oct. 2018.

"The new wave Indian MSME-An action agenda for growth - KPMG." https://assets.kpmg.com/content/dam/kpmg/pdf/2016/03/The-new-wave-Indian-MSME.pdf. Accessed 5 Nov. 2018.

"The Rise in Internet Penetration and the Changing Face of Digital India." 27 Jan. 2015, http://www.iamwire.com/2015/01/rise-internet-penetration-changing-face-digital-india/108808. Accessed 26 Oct. 2018.

"to Download File - IBEF." https://www.ibef.org/download/IT-_ITeS-Report-Apr-20181.pdf. Accessed 5 Nov. 2018.

"Top 10 operational impacts of the GDPR: Part 4 - Cross-border data ...." https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/.Accessed on 15 Nov.2018.

“Traffic Congestion and Reliability: Linking Solutions to Problems” https://ops.fhwa.dot.gov/congestion_report_04/executive_summary.htm. Accessed on 15 Nov 2018.

"Treaties and Agreements - US Department of State." 7 Mar. 2012, https://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm. Accessed on 15 Nov.2018.

"TODAYonline | Data protectionism: the growing menace to global ...." 20 May. 2018, https://www.todayonline.com/world/data-protectionism-growing-menace-global-business. Accessed 26 Oct. 2018.

"Tracing the Economic Impact of Regulations on the Free Flow of Data ...." 30 May. 2016, https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf. Accessed 26 Oct. 2018.

"Unleashing Internal Data Flows in the EU: An Economic Assessment ...." http://ecipe.org/app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf. Accessed 15 Nov.. 2018.

"Vietnam National Assembly Passes the Law on Cybersecurity - Lexology." 15 June. 2018, https://www.lexology.com/library/detail.aspx?g=843a0ed4-5583-434f-8f56-fc206f14c770. Accessed on 15 Nov. 2018.

“What is Data Localisation ?-Definition from Technopedia” https://www.techopedia.com/definition/32506/data-localization. Accessed on 15 Nov 2018.

"What is Data Ownership? - Definition from Techopedia." https://www.techopedia.com/definition/29059/data-ownership. Accessed 4 Nov. 2018.

"What are executive agreements under the Cloud Act ? - Mathias Avocats." 25 Jun. 2018, https://www.avocats-mathias.com/actualites/executive-agreements-cloud-act. Accessed 2 Nov. 2018.

"WHITE PAPER OF THE COMMITTEE OF EXPERTS ON A ... - MeitY." 4 Nov. 2017, http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf. Accessed 31 Oct. 2018.

"White Paper on Data Protection framework for India - Public ... - MeitY." 18 Dec. 2017, http://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited. Accessed 1 Nov. 2018.

"Why India should let its citizens' data roam free - The Economic Times." 14 Sep. 2018, https://economictimes.indiatimes.com/news/economy/policy/why-india-should-let-its-citizens-data-roam-free/articleshow/65803440.cms. Accessed 26 Oct. 2018.

"World Bank Document - Open Knowledge Repository." https://openknowledge.worldbank.org/bitstream/handle/10986/24866/WPS7785.pdf. Accessed 26 Oct. 2018.

"Telecom Sector Needs More Than FDI - India Real Time - WSJ." 18 Jul. 2013, https://blogs.wsj.com/indiarealtime/2013/07/18/telecom-sector-needs-more-than-fdi/. Accessed on 14 Nov. 2018.