IAMAI
Internet And Mobile Association Of India

ICRIER

Economic Implications

of Cross-Border Data Flows

November, 2019

AUTHORS:

Rajat Kathuria, Mansi Kedia, Gangesh Varma and Kaushambi Bagchi

Economic Implications

of Cross-Border Data Flows

Disclaimer

Opinions and recommendations in the report are exclusively of the author(s) and not of any other individual or institution including ICRIER. This report has been prepared in good faith on the basis of information available at the date of publication. All interaction and transactions with industry sponsors and their representatives have been transparent and conducted in an open, honest and independent manner as enshrined in ICRIER Memorandum of Association. ICRIER does not accept any corporate funding that comes with a mandate research area which is not in line with ICRIER's research agenda. The corporate funding of an ICRIER activity does not, in any way, imply ICRIER's endorsement of the views of the sponsoring organization or its products or policies. ICRIER does not conduct research that is focused on any specific product or service provided by the corporate sponsor.

Table of Contents

List of Tables

List of Figures

Acknowledgements

We are grateful to our project sponsor, IAMAI, for giving us the opportunity to undertake this study that deep dives into what has become a passionately debated policy piece of India's digital economy. A study of this scale and nature would not have been possible without the cooperation of industry stakeholders, whose inputs have shaped the analysis presented in this study. Given the sensitivity of the issue, we are grateful for their support and participation in helping us build the arguments and economic analysis. We are thankful to Dr. Arpita Mukherjee for her generosity with time in arranging meetings with important stakeholders. We extend our gratitude to MRSS and Spectrum Research in implementing the enterprise survey. We are immensely grateful to our former colleague, Vatsala Shreeti for her extensive help while working with challenging models and data. We are grateful to our interns, Alexandra Tristant and Tanay Katiyar for their timely assistance with data collection and visualisation. We are especially grateful to our colleague, Isha Suri, whose expertise in law was pivotal in the interpretation and understanding of data protection laws around the world. We are extremely grateful to Kreativ Street for helping with the graphics, data visualisation and overall design of the report. The report in its current form would not have been possible without their creativity, careful detailing and tireless efforts. Last, but not the least, we are grateful to our colleagues at ICRIER for providing a stimulating environment which makes such research possible. All errors remain our own.

Executive Summary

Cross-border data flows have become indispensable to international trade. Data is experiencing a new found and unprecedented role as an input to global trade and commerce, impacting not only the information technology (IT) sector, but also traditional industries. To cater to this upsurge, global internet bandwidth increased from a mere 56 Gbps in 1999 to 393 Tbps in 2018, an annual increase of an astonishing 59.1 percent (CAGR). Between 2014 and 2018, Africa experienced the most rapid growth of international internet bandwidth at a compounded annual growth rate of 45 percent. During the same period, India's international internet bandwidth increased by 62.7 percent per annum.

While the rapid increase in data flows has contributed to growth and socio-economic transformations, it has also amplified policy questions related to anti-trust conduct, inequality, privacy, data security and surveillance. Some of these questions are driven by the capacity, integrity and commitment of private businesses to secure users' personal data they collect and utilize for business purposes. Additionally, policy making by some governments has sparked debate on issues of data sovereignty and citizens' privacy. Given that international legal and regulatory regimes develop at a much slower pace than technology, some countries have adopted regional rules and guidelines or their own national policies on data regulation.Governments are raising concerns about the safety of data routed through and stored outside their jurisdictions. *Data localisation* policies require data pertaining to citizens of a country to be processed and/ or stored within its jurisdiction; moreover, inflexible mandates can completely restrict the flow of data outside the country.

Data localisation most pithily refers to measures "*that encumber the transfer of data across national borders*". The rationale for data localisation includes an inward outlook on commerce, protection of rights of data subjects and law enforcement challenges in order to guard against foreign surveillance. The economic motivation for data localisation relates to attracting investment, fueling innovation and creating competitive advantage for domestic companies. Countries localising on grounds of privacy argue that in the absence of other comprehensive data sharing regimes between countries, localisation is the only practical option available to governments to protect the privacy of their citizens. Data localisation is also cited as a response to the currently broken Mutual Legal Assistance Treaty (MLAT) regime that provides law enforcement agencies (LEAs) access to data for criminal investigations.

While several countries across the world have adopted some measures for regulating data flows, others are contemplating its introduction. In India, the recent debate around data localisation emerged in the backdrop of the Justice Srikrishna Committee Report, and the draft Personal Data Protection Bill, 2018. Although the formulation of India's overarching privacy framework is underway, different sectoral regulators proposed measures that affect data management and flows for businesses in the private sector. The most prominent and strict of these was RBI's notification on localisation of payment systems data that was implemented without much consultation. The most recent proposal to include provisions on localisation was the draft e-commerce policy. A revised draft of this policy was introduced in February 2019. The new draft retained localisation requirements. However, India's Commerce Minister recently announced that data localisation norms would form a part of the Ministry of Electronics and Information Technology (MeitY)'s policy mandate and is likely to be dealt with, in the Personal Data Protection Bill.

This report builds on the recent literature on data localisation to provide a reflective view on the economic implications of the existing and proposed localisation measures in India. The study captures the economic impacts of data localisation by presenting both domestic and global business models and the potential impact on India's international trade. Localisation measures more often than not transcend economic considerations. A blanket assessment on the need for or efficacy of data localisation, is therefore not within the scope of this study. The focus of this study is restricted to the economic dimension.

For the macro-economic assessment in this study, we estimate the impact of cross-border data flows on international trade. We hypothesise that cross border data flows positively impact India's foreign trade. Towards this objective, we use an *augmented gravity model* of trade. The estimation is based on a panel data set of trade between India and 37 partner countries over the period 2014 to 2018. Our estimation produces significant and consistent results confirming the stated hypothesis. Box ES.1 summarises the results.

Box ES.1: Key Results from the Econometric Estimation

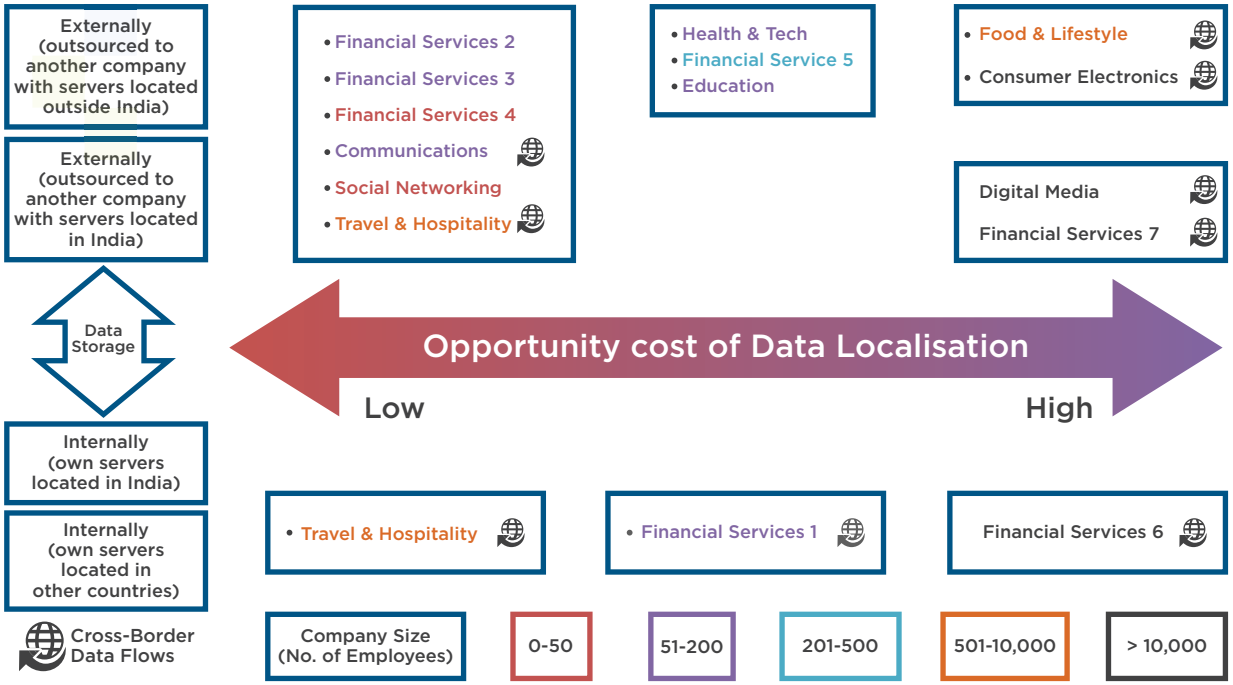
A 1 percent increase in international internet bandwidth leads to an increase of US$ 696.71 million in total volume of goods trade for India. From 2016-17 to 2017-18, total international internet bandwidth in India increased by 35 percent, thus leading to an increase of approximately US$ 24 billion in total volume of goods trade. During the same period, the absolute increase in India's total volume of trade was approximately US$ 202 billion. Therefore, approximately 12 percent of the growth in India's total volume of trade was on account of increase in international internet bandwidth.

The magnitude of the multiplier could be higher when bilateral services trade data is included in the model, as much of the trade in services, Mode 1 services in particular, is facilitated by the internet.

Between 2014 and 2018, the compounded annual growth rate (CAGR) of international internet bandwidth was 62.7 percent for India. Should the projected rate of growth for international internet bandwidth be at the existing CAGR, India's total volume of goods trade is likely to increase by US$ 43 billion annually, on account of increase in internet bandwidth.

While the macro-economic estimate quantifies the impact of cross-border data flows on foreign trade in India, it does not capture the character of impacts across sectors and business types. Evidence shows that costs of data localisation are likely to be the highest for sectors such as communication and financial services. In India, financial services witnessed the first explicit mandate for local data storage. We use our analysis from fifteen in-depth case studies covering online businesses across manysectors to explain the impacts of data localisation. Figure ES.1 presents the opportunity cost of data localisation for the fifteen companies included in our case study analysis. The impact of data localisation, we find, is not uniform across sectors, and also varies between companies within the same sector. Box ES.2 summarises the key findings from the case study analysis.

Figure ES.1: Opportunity Cost of Data Localisation



In addition to the case studies, using a diversified sample that covers both online and traditional businesses, integral to India's economy, also forms a part of our impact analysis. The survey sample includes traditional firms in the manufacturing and services sector, in addition to typical examples from the digital economy. The survey reinforces our conclusion on the impact of data localisation on businesses across sectors. The impacts vary by the size of the company, the sector of operation, the choice of markets, business models, etc. Impacts also vary by the nature and location of the firm. The commonly held perception that domestic companies stand to benefit from data localisation policies is simply not correct. Our analysis shows that there are negative cost implications for domestic companies as well. Therefore, an inclusive and comprehensive policy discourse will better serve the long-term interests of stakeholders and the Indian economy.

Box ES.2: Findings from the Case Study Analysis

I. Data Regulations and the Emerging Data Storage Ecosystem in India

- There is a pattern of migration from managed data servers to leased cloud services, and migration from cloud services located on foreign soil to cloud services in India. The former trend is on account of the agility and ease of scalability provided by cloud services while the latter is in anticipation of localisation requirements likely to emerge in the future.
- While India may not have been a natural choice for most companies to store and process data, many companies interviewed as a part of the study reported storing their data in India as a pre-emptive measure for policies likely to be introduced in the future.
- The services of foreign cloud operators have scaled manifold in India. Indian cloud service providers, however, continue to lag behind global service providers such as Amazon, Google, Microsoft etc. both in terms of quality and availability of sophisticated features as well as cost effectiveness. The growth in domestic IT infrastructure is being organically driven by India's push for IoT systems, the mushrooming of startups with internet-based delivery models and the growing adoption of big data analytics and artificial intelligence.

- Data management for companies in the financial services sector is particularly complex. The nature and volume of data collected by financial services companies expose them to additional compliance requirements, especially with respect to policies on sensitive and personally identifiable data.

II. Data Localisation – Implications on Cost, Innovation and Privacy

- Since most mature financial services companies use integrated global architectures for data management, localisation is likely to impair their fraud detection and anti-money laundering systems. The fraud detection systems could be weakened leading to a ten-fold increase in fraud losses in India. Moreover, the cost of compliance is not likely to be one-time. The costs of maintaining and upgrading these systems, unique to each company, will be recurrent and significant.
- A food and lifestyle company of Indian origin currently using cloud services hosted in Singapore feared that the applications provided by their existing cloud service provider may not be all available at the same cost in India. While it may be difficult for them to pass on these costs to consumers in a hyper competitive digital services market, business partners are likely to bear the brunt of this increased cost.
- Most small and medium sized enterprises of Indian origin operating exclusively in India, reported a one-time cost of migration to local data centers, if at all, and no ongoing impact from localisation. In the short to medium run, these companies might have to suffer from the lack of adequate features available in the Indian data centres.
- Several companies reported that forced development of data centers is likely to increase costs for businesses, as the cost of other supporting infrastructure such as power is significantly higher in India.
- Despite incurring moderate costs, some companies were of the belief that data localisation would lead to lesser latency if servers were located in India.
- While data localisation might lead to a competitive advantage for domestic companies in the short run, vis-à-vis their foreign competitors; in the long run, such an entry barrier might prove detrimental as innovation would be thwarted and the market will become less competitive.
- For companies that want to enter the Indian market, increased costs of localisation might act as an entry barrier. This is particularly true for foreign SMEs and startups for whom this cost might be significant.
- Most stakeholders agreed that the location of data is inconsequential to improving privacy outcomes.
- Companies also feared global retaliation against India's localisation measures. Such measures can adversely impact India's domestic firms, such as Indian IT companies which rely on global markets.

III. Policy Perspectives

- The perceived benefits, such as growth of the data economy and indirect job creation, accruing from data localisation can be achieved through alternate means that are less disruptive for global businesses.
- The lack of clarity on guidelines make it difficult for firms to prepare for compliance with localisation norms, as pointed out by stakeholders with respect to RBI's 2018 Directive. The draft Personal Data Protection Bill in its current form is also vague about the classification of data. Such ambiguities increase compliance costs and must be addressed.
- In order to meet government objectives mid-way, several alternatives to localisation were proposed by the companies. Data mirroring and exchange through bilateral and plurilateral mechanisms were proposed as alternatives to hard localisation.

The report is an attempt to present objective evidence on a subject that has tended to become impassioned because of the conflicting and divergent positions of stakeholders. It is imperative to note that this study is not a binary assessment of whether data localisation is good or bad. To repeat, the focus is primarily economic with the additional aim to derive a set of policy recommendations that strike a balance between achieving the objectives of data localisation and minimising its unintended consequences. Box ES.3 provides the policy recommendations.

Box ES.3: Policy Recommendations

Encourage bilateral or plurilateral data transfer arrangements and soften data localisation measures through mirroring of select datasets: In addition to reforming the MLAT System, it would be useful for India to explore bilateral or plurilateral data transfer arrangements, such as certification. Data transfer mechanisms like the US-EU Privacy Shield (bilateral) and APEC CBPR (multilateral) help ensure compliance with local laws, even when data is transferred outside the jurisdiction. India could also consider mirroring of critical datasets. Mirroring requirements allow for free flow of data while also providing local access of data to relevant authorities, with relatively lower cost implications.

Encourage international regulatory cooperation: Instead of mandating blanket localisation, countries could explore agreements or memorandums of understanding (MOU) between specific regulators across the globe to address specific issues of access to data, monitoring and safeguarding consumers' welfare and interests.

Minimise policy overlap: India is currently witnessing a host of proposed sectoral localisation measures that often overlap with existing policies, such as the Draft E-Commerce Policy, the draft e-pharmacy regulations etc. This results in potential overreach and over-regulation of the industry resulting in regulatory uncertainty.

Institutionalise consultative and transparent policy making: When policy making is consultative and transparent it is easier for stakeholders to understand the motivations, objectives and thinking that goes into formulation of the concerned policy. Moreover, regular communication enables them to comply better and share efficient alternatives.

Enable the overall digital ecosystem instead of forced data localisation: In India's current economic state, building local data centers may misallocate valuable resources resulting in loss of efficiency and suboptimal choices for global businesses. Forced data localisation, if at all, will help achieve the stated objectives at higher costs. On the other hand, policies that focus on the development of the overall ecosystem will organically invite localisation as businesses will find it more profitable and efficient to operate from India.

Evaluate risks of retaliatory measures and the potential fragmentation of the internet: Retaliatory measures from other countries would not only impact the consumers but also risk fragmentation of the global internet. The fragmentation of the internet, would revert the benefits of globalisation and isolate countries such as India, from the global value chains that make the data economies of today.

Assess costs of delayed availability of latest services and updates in India and the negative impact on innovation: Many global businesses would have to maintain dual set of infrastructures to comply with localisation measures in India. As a result, new services rolled out globally will need to be separately launched in India through Indian infrastructure. This could result in delays, and inadvertently affect consumer choice and competition in the market.

Conduct Regulatory Impact Assessments (RIAs), security audits and vulnerability assessments before policy development and implementation: RIAs are commonly conducted by many regulators of various sectors in different countries. They could help policy makers by providing evidence on the impacts of an implemented policy, Further, data security audits and vulnerability assessments both for private businesses and public sector organisations, can help ensure privacy and protection of data. This could be a viable alternative to sweeping data localisation measures.

Strengthen the overall cybersecurity framework as data localisation impedes globally coordinated security measures and fraud risk analysis: The utility of big data, and learning from global patterns of security threats, fraud etc. have led to improved cybersecurity practices, prevention of fraud, and risk analyses. Fragmenting the datasets would entail alterations in these processes. Moreover, in cases where such alterations are not possible, then the aforementioned practices would have to be foregone.

Economic Implications of Cross-Border Data Flows

1. Introduction

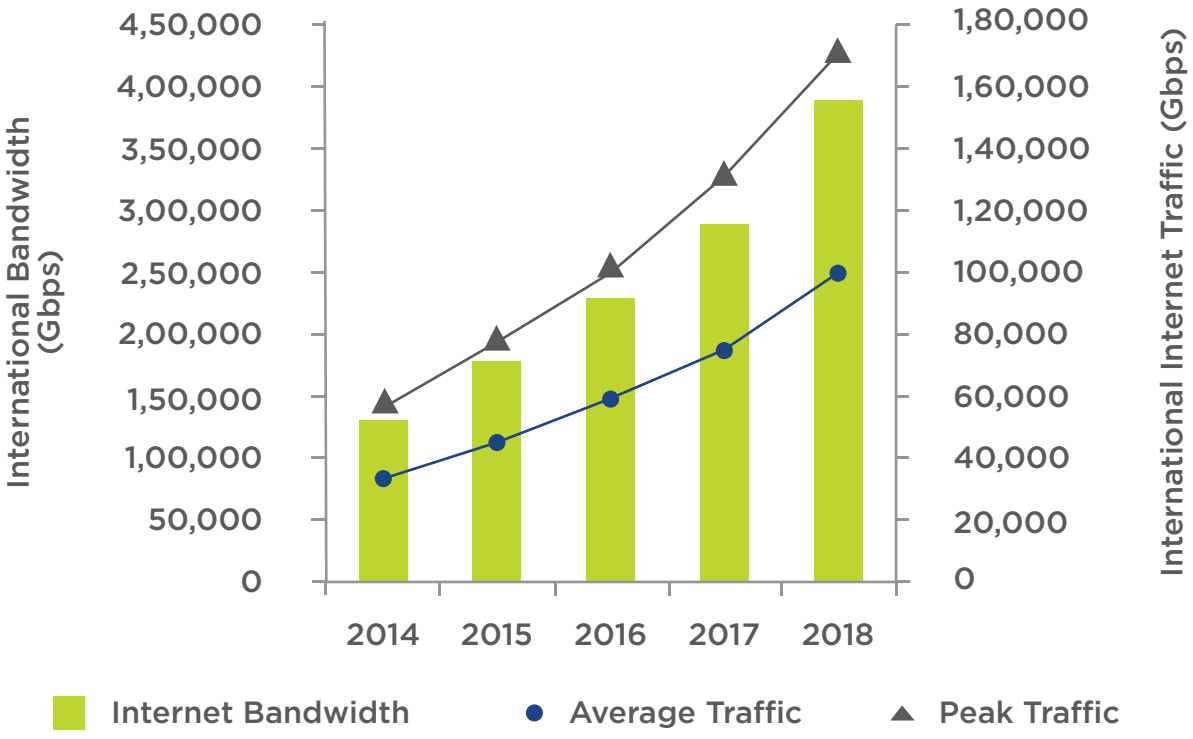
The impact of technology and innovation can be likened to the "gale of creative destruction", a metaphor immortalized by Joseph Schumpeter in 1934.The unceasing innovations in information and communication technology (ICT) have had Schumpeterian impacts, in that, these have transformed businesses, including their models of operation, organisational processes, institutions and skills as predicted.[1] ICT is now widely regarded as a general-purpose technology (GPT) because of itsubiquitous deployment. Production of information, it is argued, involves high fixed costs but low marginal costs.[2] Instantaneous access to information, a departure from the old order of lagged flows, has significantly lowered search costs. As information on nearly anything is simply a click away, the role of geographical distance and the cost of transportation of digital goods has become negligible.[3] Varian and Shapiro define information in the digital age, as anything that can be encoded in a stream of bits. In common terminology, it is known as digital data, which is the lifeblood of the modern digital economy. The digital age has changed and challenged several traditional industries, pivoting competitive advantage primarily on knowledge, information and innovation.

Enormous volumes of data are being generated every second.[4] According to IDC, close to 5 billion consumers interact with data on a daily basis and this number is likely to rise to 6 billion by 2025, accounting for nearly 75 percent of the world's population and each connected person will have at least one data interaction every 18 seconds.[5] IDC predicts that global volume of data will grow from 33 zettabytes in 2018 to 175 zettabytes in 2025 and 49 percent of the world's data will be stored in public cloud environments.[6] With enormous amounts of data at their disposal, businesses are now equipped to capture value from analytics. Personal data is being collected and analysed to better understand customer preferences. With consumers' willingness to pay for personalisation,[7] the rise of big data is evidence of how firms are monetising data to not only reduce costs butproduce targeted products and services.[8] Research has shown that businesses which depend on data-driven decision-making, perform better in terms of output and productivity.[9]

1. Brynjolfsson, Erik, and Andrew McAfee. Race against the machine: How the digital revolution is accelerating innovation, driving productivity, and irreversibly transforming employment and the economy. Brynjolfsson and McAfee, 2012.
2. Shapiro, Carl, and Hal R. Varian. Information rules: a strategic guide to the network economy. Harvard Business Press, 1998.
3. Ibid
4. Marr, B. "How much data do we create every day? Forbes (2018) Available at https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/
5. "The Digitization of the World From Edge to Core". IDC, 2018.
6. Ibid
7. OECD (2018), Personalized Pricing in the Digital Era. Available at https://one.oecd.org/document/DAF/COMP(2018)13/en/pdf
8. "The Rise of Data Capital", MIT Technology Review Custom + Oracle. Available at http://files.technologyreview.com/whitepapers/MIT_Oracle+Report-The_Rise_of_Data_Capital.pdf
9. Brynjolfsson, Erik, Lorin M. Hitt, and Heekyung Hellen Kim. "Strength in numbers: How does data-driven decisionmaking affect firm performance?." Available at SSRN 1819486 (2011).

The importance of data has also risen in ranks as an input to global trade and commerce, impacting not only the information technology sector, but also traditional industries.[10] Cross-border data flows have become indispensable to digital trade.[11] This trend also reflects in the growth of global internet bandwidth which has increased from a mere 56 Gbps in 1999 to 393 Tbps in 2018.[12] Between 2014 and 2018, Africa experienced the most rapid growth of international internet bandwidth at a compounded annual growth rate (CAGR) of 45 percent, followed closely by Asia and Middle East which recorded a 41 percent CAGR.[13] The corresponding growth in India was dramatically higher. During the same period, India's international internet bandwidth increased by 62.7 percent, average and peak internet traffic increased by 51.08 percent and 55.74 percent respectively.[14] Figure 1.1 and Figure 1.2 provide trends for internet bandwidth and traffic at the global and India level respectively. Content providers have become a big source of international bandwidth, accounting for 49 percent of the international bandwidth use in 2017, outpacing the capacity deployed by internet backbone operators in recent years[15].

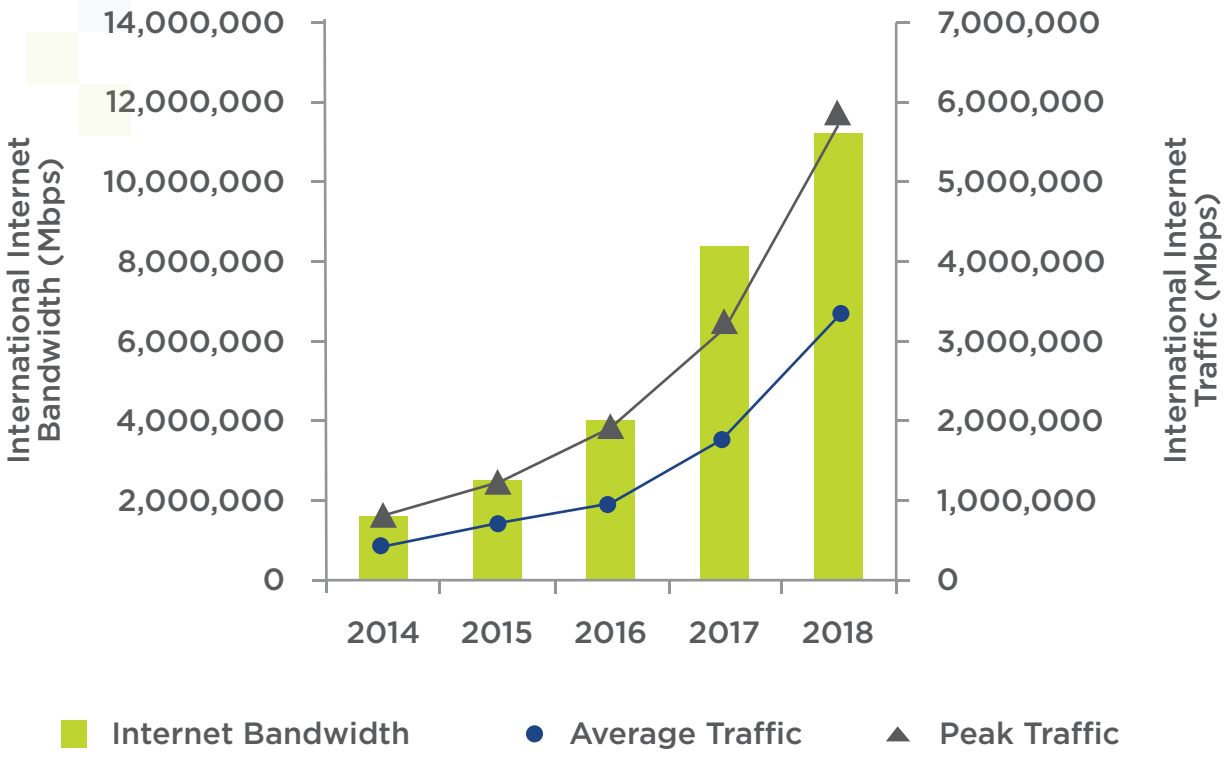
Figure 1.1: Global Internet Bandwidth and Internet Traffic



Source - TeleGeography

10. Cory, Nigel. Cross-border data flows: Where are the barriers, and what do they cost?. Information Technology and Innovation Foundation, 2017.
11. The United States International Trade Commission (USITC) defines digital trade as the delivery of products and services over either fixed-line or wireless digital networks.
12. Global Internet Geography, Capacity and Traffic Trends, TeleGeography, 2018
13. Ibid
14. TeleGeography GIG Database
15. Op Cit, 12

Figure 1.2: India's International Bandwidth and Internet Traffic



Source - TeleGeography

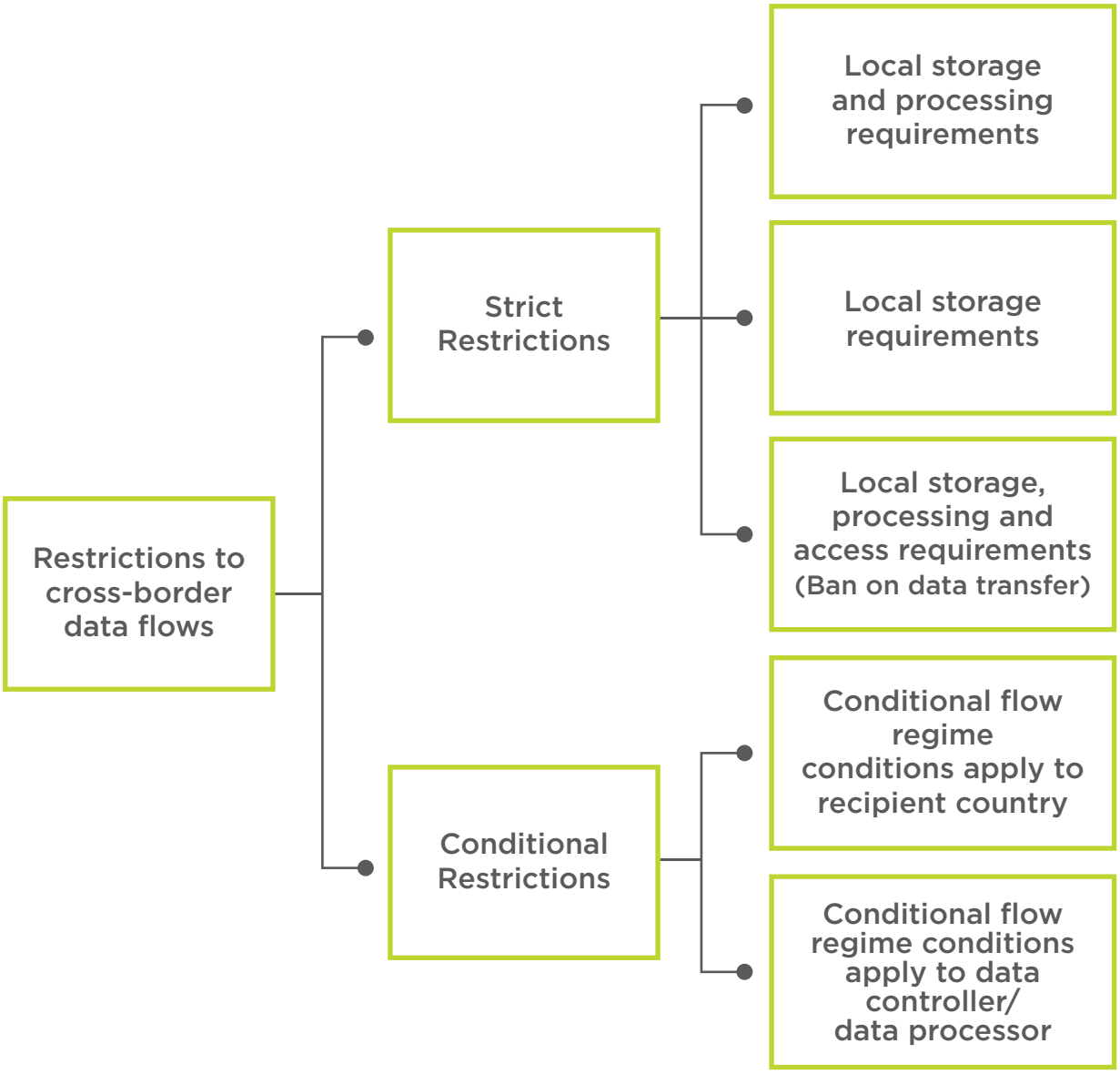
The movement of constant, real-time information, often across borders, is critical to many technologies including cloud computing, machine-to-machine communication, etc.[16] Cross border data flows improve productivity and enable the creation of efficient markets. According to McKinsey Global Institute (MGI), all types of tangible and intangible flows have raised the world GDP by 10.1 percent, over the past decade. This value amounted to US$7.8 trillion in 2014, of which, data flows accounted for US$ 2.8 trillion. However, the promise and dynamism of the data economy is not without challenges. Burgeoning volumes of data, its evolving nature and utility have led to fresh policy challenges. Some of these questions are driven by the capacity, integrity and commitment of private businesses to secure users' personal data that they collect and leverage for business purposes. Additionally, policy making by some governments has also sparked debates on issues of data sovereigntyand citizens' privacy. Seeing a remarkable rise in the use of data, particularly the use of personal data, many countries have responded by introducing either new data regulations or adapting their existing data regulations and policies to the current environment.[17]

In the absence of a cohesive and harmonious international legal regime, several countries have developed their own national policies or legislations. Given that international legal regimes develop at a much slower pace than technological surges, some countries have adopted regional rules and guidelines. While these regulate specific geographies and jurisdictions, they also inspire the development of both national and international legal regulations.[18]

16. Unleashing the benefits of free flow of data, Telenor 2018, https://www.telenor.com/wp-content/uploads/2018/04/201804_Telenor-external-FoD-position_FINAL.pdf
17. See Appendix 1 for list of Proposed and Existing Data Localisation Measures around the World
18. Examples include the development of the European Union's General Data Protection Regulation, and APEC Cross Border Privacy Rules. More recently, further intention to develop global and regional frameworks can be seen in the G20 Osaka Declaration.

Governments are raising concerns about the safety of data routed through and stored outside their jurisdictions. *Data Localisation* mandates that data pertaining to the citizens of a particular country be processed and/ or stored within its jurisdiction and restricts the flow of data outside the country. In the context of trade, restrictions to cross-border data flows can be considered as a form of non-tariff barrier[19] that increases the cost of international trade. The classification of restrictions on cross-border data flows has been mapped by Ferracane (2017). In this report we analyse data regulation including data localisation policies adopted in India and its potential economic impact.

Figure 1.3: Classification of Restrictions to Cross-Border Data Flows



Source – Ferracane (2017)

19. https://fas.org/sgp/crs/misc/R44565.pdf

1.1 Scope of the Study

This report builds on the recent literature on data localisation to provide a reflective view on the economic implications of the existing and proposed localisation measures in India. The study captures the economic impacts of data localisation by presenting both domestic and global business models and the potential impact on India's international trade. Localisation measures more often than not transcend economic considerations. A binary assessment on the need for or efficacy of data localisation, is therefore not within the scope of this study. The focus of this study is restricted to the economic dimension and as we show, it will depend on several factors. The rest of the report is organised as follows. Section 2 discusses the history of regulations on cross-border data flows and localisation measures adopted by countries including India. In section 3, we provide a quantitative estimate for the impact of cross-border data flows, measured using international internet bandwidth, on India's international trade. In Section 4 we summarise our findings from fifteen in-depth interviews with online businesses that span across different sectors of the economy. The interactions provide insights on the nature and use of data in business processes and the potential impacts from localisation mandates. Section 5 uses survey responses for over 200 enterprises in India to understand and analyse their data management practices including their perceived impact from localisation measures. Section 6 summarises the analysis and makes recommendations for policy.

2. History of Regulations on Cross Border Data Flows and Data Localisation

The internet was designed to be a decentralised network of networks that grew to its current significance without being controlled or owned by a single country, company or individual. The advancement in computing technologies and their ability to remotely process large volumes of data created new opportunities for both commerce and communications to expand beyond limited geographies. Several multinational enterprises now operate using globalised business models that are based on sophisticated data-fed algorithms. While such models massively enhance efficiency, the volumes of data collected in the process, especially those that are personal and identifiable in nature, raise concerns over its ownership and transfer. This has led countries to adopt laws that protect the data of their citizens and propose international frameworks that minimise jurisdictional conflict.[20] The first attempt at harmonization can be traced back to regulations on trans-border data flows in Europe in the 1970s. In the 1980s, the OECD formulated guidelines on data flows, data protection and privacy.[21] The internet has however transformed since then and compelled another look. In an era of hyper personalization, businesses have become completely data driven reinforcing the need for a mature and harmonious legal regime to govern its use and flow.

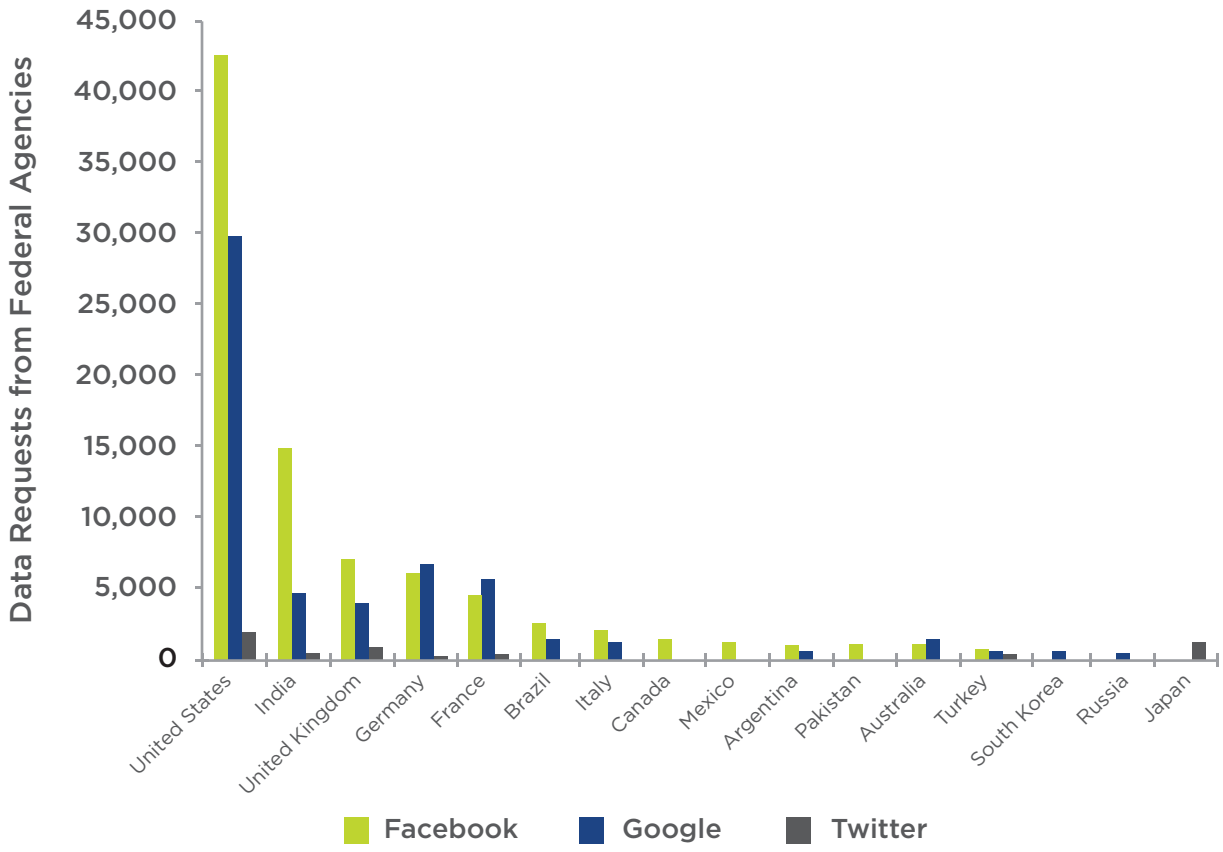
Some consider that the most recent trigger for stringent regulation of data flows was Edward Snowden's revelations on the NSA's surveillance programs in the US which included monitoring the communications of foreign citizens and foreign governments.[22] Following this, several countries proposed regulations to restrict data flows, citing concerns related to the privacy and security of their citizens.[23] Many of these proposals, however, remained contemplative and were not backed by concrete legislative actions.

Governments' fears have been magnified by the onslaught of data breaches which have compromised the security of citizens' sensitive personal data. The World Economic Forum's Global Risk Report 2018 finds that the threat of cyber-attacks and cyberwarfare is only behind extreme weather events and natural disasters in terms of events likely to cause disruption in the next five years. The average cost of a data breach in 2019 was estimated to be $3.92 million[24]. v

20. UNCTAD (2016)
21. Kuner, Christopher. "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. OECD Digital Economy Papers, 187, (2011)
22. Konstantinos Komaitis (2017) The 'wicked problem' of data localisation, Journal of Cyber Policy, 2:3, 355-365, DOI: 10.1080/23738871.2017.1402942
23. Ibid, also see Sargsyan (2016)
24. https://digitalguardian.com/blog/whats-cost-data-breach-2019

According to a report by the Identity Theft Resource Centre, the reported number of exposed consumer records that contained sensitive personally identifiable information had increased by 126 percent during 2017 and 2018. The expansion of the digital economy and theuse of the internetfor communications has naturally led to themisuse of online spaces. This is reflected in the rising number of data requests from governments and law enforcement agencies on cyber-crimes and other criminal investigations. Figure 2.1 shows the number of data requests that have been made by federal bodies to Facebook, Google and Twitter for select countries in the first half of 2018. India ranks second to the United States in this regard. An obvious but hard question is whether localisation of data is the appropriate measure to address these concerns.

Figure 2.1: Data Requests from Federal Agencies



Source – Statista

Data localisation most pithily refers to measures "*that encumber the transfer of data across national borders*". The impulses for data localisation include an inward outlook on commerce, protection of rights of data subjects and law enforcement challenges in order to guard against foreign surveillance. The economic drivers for data localisation relate to attracting investment, fueling innovation and creating competitive advantage for domestic companies. A review of regulating cross-border data flows reveals two default positions – (i) data flows are permissible with the possibility of regulation and (ii) data flows are not permissible without a legal basis[25].

25. Kuner (2011)

Proponents of data localisation argue that free data flows may be antithetical to new pathways of growth - the current data regime relies on the extensive collection, processing and storage of data for digital intelligence from the South by the corporations of the global North.[26] Thus, according to them, in order to harness the power of digital intelligence, developing countries need to enact interventionist state policies to promote local over foreign platforms.[27] Further, financing an 'Internet plus' digital industrialisation strategy for big data, cloud and the Internet of Things, and enabling smaller enterprises to build their presence online are part of the strategy mix.[28]

Countries localising on grounds of privacy argue that localisation is the only practical option available to governments to protect the privacy of their citizens, in the absence of other comprehensive data sharing regimes between countries.[29] Data localisation is also cited as a response to the currently broken Mutual Legal Assistance Treaty (MLAT) regime that provides law enforcement agencies (LEAs) access to data for criminal investigations.

On the other hand, several economists and legal scholars argue that data localisation is a modern-day trade barrier. Data localisation will entail an overhaul of the core architecture of the internet. Where localisation requirements are already mandated, data may have to be routed through more congested networks, which would reduce systemic efficiencies. Cutting off data flows or making them more costly not only puts foreign or multinational firms at a disadvantage,[30] but shields local or domestic companies from global competition, and suppresses their ability to participate in the global digital economy in the long run.[31] Moreover, data localisation will centralise data storage, making it more vulnerable to breaches and prevent efficiency and security improving measures like 'sharding'.[32] It has also been argued that localisation will thwart innovation and impact consumers' access to services in the long run. With respect to foreign surveillance, it is argued that the scale and potential of surveillance capabilities is so enormous that perhaps the only way to avoid it may be to not have the data connected to the internet.[33] Moreover, security experts argue that data localisation would degrade rather than improve data security in countries and make surveillance of citizens by domestic governments easier.[34]

2.1 Data Localisation around the World

Localisation of data can assume two broad forms – *localised data hosting* where hosts are compelled to store data about users in a country within its geographical jurisdiction; and *localised data routing* where service providers are compelled to route data packets between users located in a country through networks located only within the country's geographical jurisdiction. The scope of implementation of these policies can vary – localisation can either be explicitly required by law or be the outcome of other restrictive policies that make cross-border transfer of data infeasible. This includes for example the requirement that companies store a copy of the data locally which automatically entails local processing of data; or mandating individual or government consent for data transfers across borders.

Data regulations derive from the unique legal traditions and culture of a country. For example, laws in the European Union are founded on legally-binding human rights instruments while in the APEC region, the measures are based more on realising the benefits of e-commerce.

26. Gurumurthy, Vasudevan and Chami (2017)
27. Ibid
28. Ibid
29. Panday (2017)
30. USITC (2017)
31. IAMAI (2016); UNCTAD (2016)
32. Sharding is a process in which rows of a database table are held separately in servers across the world in such a way that shards provide enough data for operations but does not suffice for the re-identification of the individual.
33. Chander and Le (2014)
34. Hill, Jonah. "The growth of data localization post-snowden: Analysis and recommendations for us policymakers and business leaders." In The Hague Institute for Global Justice, Conference on the Future of Cyber Governance. 2014.

EU's General Data Protection Regulation (GDPR) implemented in May 2018 is the most comprehensive data protection policy in recent times and is quickly becoming a reference model for other countries. It has been designed to harmonise data privacy laws across EU and provide greater protection to individuals' data.[35] The GDPR while regulating access to data does not mandate local storage requirements. The regulation covers both personal and sensitive personal data.[36] GDPR provides individuals with better control and access to their data.[37] It also makes companies accountable for the handling of individual's personal information. Compliance with GDPR requires companies to define data protection policies, conduct data protection impact assessments and document their data processing mechanisms.[38]

A contrasting exampleof a narrowly focused local storage requirementis Australia's My Health Records Act of 2012. It requires all electronic health records to be stored in local data centres. Electronic health records that are personally identifiable cannot be held or processed outside Australia.[39] An amendment in 2018 restricted the operator of My Healthcare Records Systemto disclose any data without a judicial order or the patient's consent, even to law enforcement or government agencies.[40] Germany has also mandated storage and processing of public sector data on 'Bundescloud', a policy that is in sharp contrast to its otherwise open approach to foreign trade. Notably, several countries approach localisation with specificity and target either critical or sensitive data, however the definitional scope varies in their legislations.

China probably has one of the most stringent data localisation regimes in the world. For example, articles 24 and 61 in the law require all telecommunication service providers and instant messaging services to request real name registration from its users and share data with the government thereafter, for purposes of law enforcement.[41] Since 2011, China's Central Bank has mandated that financial information collected in China's territory be stored, processed and analysed within its jurisdiction.[42] While these are sector specific requirements, anoverarching cybersecurity policy was proposed with broader scope and applicability. As per the draft policy, all Chinese and foreign companies have to store their data in Chinese data centres.[43] Such requirements increase concerns related to government surveillance in China. The draft measures on *Security Assessment of Cross-Border Transfer of Personal Information* was recently released for public comments in China. Although it does not includeexpress localisation requirements, it would require thorough security assessments to be conducted for cross-border transfer of data.[44]

Cushman and Wakefield's Data Centre Risk Index of 2016 ranks China as a high risk zonewith a rank of 35 out of 37 countries in terms of political stability, natural disaster risk and energy security, in addition to the more traditional factors such as cost and connectivity.[45] A report prepared by TRPC, benchmarks the performance of G20 countries in a Cross-Border Data Flows Index (CBDFI) which ranks Japan at the top, indicating that it has the least restrictive policies for cross-border data flows. US, UK and EU also rank well. India secures a rank of 11, along with Argentina. The worst performing countries, as per the index were China, Indonesia and Russia. Russia's data localisation law prevents cross-border transfer of personal data of Russian citizens and mandates its storage in servers within the country. The report finds that economic growth is enhanced by enabling cross-border flow of data which in turn facilitates businesses and institutions to benefit from global opportunities.[46]

35. https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018
36. Ibid
37. Ibid
38. Ibid
39. https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r6169
40. Ibid
41. https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/
42. Ibid
43. Ibid
44. https://www.huntonprivacyblog.com/2019/06/19/china-issues-draft-regulation-on-cross-border-transfer-of-personal-information/
45. https://verne-global-lackey.s3.amazonaws.com/uploads%2F2017%2F1%2Fb5e0a0da-5ad2-01b3-1eb8-8f782f22a534%2FC%26W_Data_Centre+Risk_Index_Report_2016.pdf
46. https://c1.sfdcstatic.com/content/dam/web/en_sg/www/documents/pdf/data-beyond-borders-report.pdf

As shown above, data localisation measures adopted by countries vary widely in the type of data, the scope of applicability, and its eventual enforcement. In Table 2.1 below we capture the types of encumbrances on cross-border data flows. We adopt Ferracane's (2017) taxonomy to list countries by type of restrictions on cross-border data flows. Ban on Transfer implies a hard data localisation regulation that completely prohibits transfer of data, where as Conditional Flows implies regulated movement of data that could be imposed with or without local storage requirements. Conditions for cross-border flow of data may include certification, regulatory adequacy, hashing or pseudonymising requirements, etc. The current restrictions on cross border flowshave been presented in two separate columns (Table 2.1) – the first captures country restrictions on overarching regulations that apply horizontally and the second for sector specific data. The analysis indicates that the predominant form of restrictions is in the nature of conditional flowswith a large number of countries limiting cross-border transfer of data to only those nations that have adequate data protection standards. With the advent of GDPR, the adequacy requirement for conditional flows has become the most preferred form of restriction on cross-border transfer of data.

Table 2.1: Regulation of Cross-Border Data Flows around the World

Country	Type of Restriction on Cross Border Data Flows (General)	Type of Restriction on Cross Border Data Flows (Sector-specific)
Argentina	Conditional flow of personal data without local storage requirement	Not applicable
Australia	Conditional flow of personal data without general local storage requirement	Local storage requirement for health records
Brazil	Conditional flow of personal data without local storage requirement	Local storage requirement for public procurement contracts
Canada	Conditional flow of personal data held by public bodies without local storage requirement	Not applicable
China	Conditional flow of personal data with local storage requirement[47]	Ban on transfer for financial data
		Local storage and processing requirement for health data
		Ban on transfer for data containing state secrets
		Local storage requirement for user data
		Local storage requirement for geolocation data
		Local storage requirement for online content publishers

47. https://www.gatewayhouse.in/data-localisation/#_ftn13

Colombia	Conditional flow of personal data with no local storage requirement	Not applicable
European Union	Conditional flow of personal data without local storage requirement (under the GDPR)	**Bulgaria** – local storage requirement for gaming data under the Gambling Act
		Denmark – conditional flow of companies' financial records and government's financial data with local storage or mirroring requirement
		Finland – local storage requirement for companies' accounting records
		France – local storage and processing requirements for public administration data
		Germany – (i) local storage requirement for tax data (ii) local storage requirement for a limited period for telecommunications data
		Greece – local storage requirement for traffic and location data in electronic communications
		Luxembourg – local processing requirement for financial data, with exceptions
		Netherlands – local storage requirement for public records
		Romania - local storage requirement for gambling data
India	Conditional flow of sensitive personal data without general local storage requirement	Local storage requirement for payments data with certain exceptions
		Proposed local storage requirement and prohibition on transfer of data generated or mirrored through the e-pharmacy portal

		The FDI Policy, 2017 prohibits transfer of subscribers' database in the broadcasting sector
		Unified Access License for Telecom, 2004, prohibits transfer of subscribers' accounting information and user information in the telecom sector
Indonesia	Ban on transfer of personal data and transaction data	Local storage requirement for financial data
		Local storage requirement for protected private data
Iran	Proposed conditional flow of personal data with local storage requirement	Local storage requirement for messaging and communications data
Kazakhstan	Local storage requirement of personal data	Local storage requirement for domestically registered domain names (.kz)
Kenya	Proposed ban on transfer of sensitive personal data. Conditional flow of personal data	Not applicable
Malaysia	Conditional flow of personal data with no local storage requirement	Not applicable
Nigeria	Conditional flow of personal data	Local storage requirement and ban on transfer of government data, with exceptions
		Ban on transfer of financial data
New Zealand	Conditional flow of personal data without local storage requirement	Local storage requirement for company records
Russia	Conditional flow of personal data with local storage requirement	Local storage requirement for financial data
		Local storage requirement for blogging sites (with more than 3000 readers)

South Korea	Conditional flow of personal data without local storage requirement	Ban on transfer of geospatial and geolocation data
Taiwan	Conditional flow of personal data without local storage requirement	Ban on transfer of communications data to Mainland China
Turkey	Conditional flow of personal data without local storage requirement	Local storage requirement for financial data
United Kingdom	Conditional flow of personal data without local storage requirement	Conditional flow of company records with local storage requirement
Vietnam	Local storage requirement with conditional flow of personal data	Conditional flow of multiple data types with local storage requirement

Source - Compiled by authors

Evidently only a handful of countries follow strict data storage requirements. Moreover, these are usually restricted to a particular type of data. Interestingly, even countries like Russia, China and Indonesia that once banned cross-border data transfers, are softening or proposing to soften the enforcement of their data localisation laws. Further, some measures presented in this table are unique to the specific strategic and political sensitivities such as the data transfer restrictions in Taiwan or the geo-spatial data localisation in South Korea. For country-wise details on localisation policies please refer to Appendix 1.

2.2 Data Localisation in India

While data localisation measures in India have recently become a topic of intense public debate, it is certainly not new. The Public Records Act (1993) and security conditions under the Unified Access License for Telecom Services (2004) are examples of localisation measures that were adopted by India several years ago to ring-fence security of sensitive data. The Public Records Act (1993) prohibits transfer of public records outside the territory of India. Under the Act, such transfers are permitted only for an official purpose or with permission from the central government.[48] The MeghRaj initiative, launched by the Government in 2014, also included data localisation as a precondition to become an empanelled cloud service provider to the government. The national cloud was designed to promote the use of cloud computing to accelerate delivery of e-services and optimise the government's ICT spending.[49]

48. See Section 4 of the Public Records Act 1993
49. https://cloud.gov.in/about.php

Several sectoral policies in India have implicitly or explicitly regulated cross border flow of data. For example, telecommunications and internet service providers who hold the Unified Access License are prohibited from transferring user information and any accounting information related to subscribers, except for international billing to any person or place outside India.[50] On the other hand, IT Rules (IT Act 2000), limit transfer of sensitive personal data bya body corporate to another entity or person, within or outside India, under the condition that the other person/ entity will be able to provide the same level of data protection that is expected under the IT rules. Additionally, such transfers are permitted only if considered necessary for the performance of an existing contract and if the person providing the information has consented to it.[51] Further, for entities to whom the Companies Act 2013 is applicable, a back-up of books of accounts and other books and papers of the company that are maintained in an electronic mode, including any records that are kept outside India, must be periodically stored in servers physically located in India.[52]

Recent debates around data localisation have been triggered by the Justice Sri Krishna Committee Report, and the draft Personal Data Protection Bill, 2018. The bill classifies data into two broad categories – personal data and sensitive personal data. They are defined in the bill, as follows:

Personal Data: Data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic trait, attribute, or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information

Sensitive Personal Data: Personal data revealing, related to, or constituting, as may be applicable – passwords; financial data; health data; official identifier; sex life; sexual orientation; biometric data; genetic data; transgender status; intersex status; caste or tribe; religious or political belief or affiliation or any other category of data specified by the Authority under section 22.

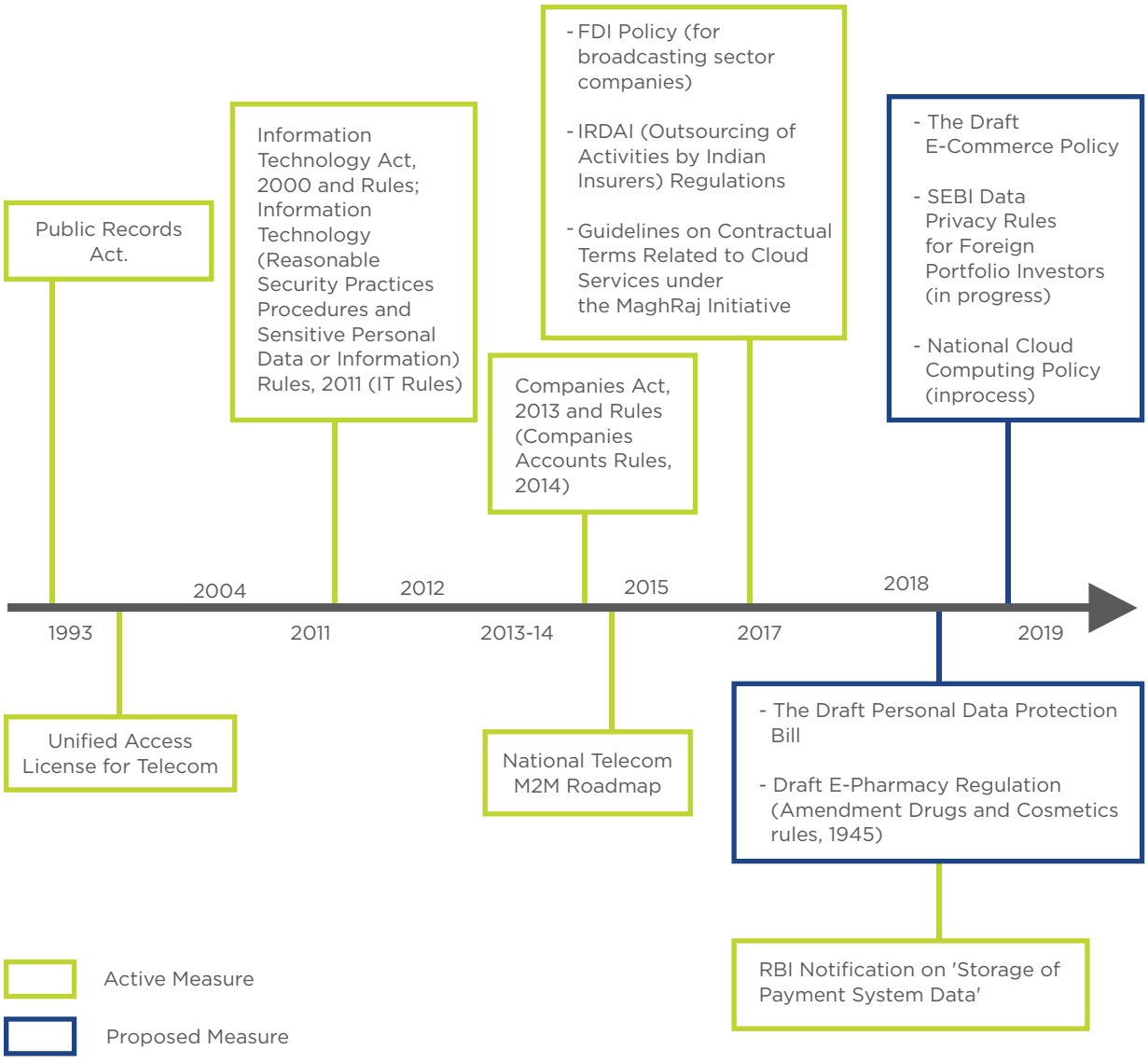
In practice, the afore mentioned data types can collectively include employee personal data, transaction and payments related data, photos and potential biometric data, passwords, data related to personal correspondence, non-differential client data that is encrypted and stored in servers, geo-location data, etc. The report discusses a potential third category, critical personal data. However, the definition and scope of this type of data has not been clarified in the bill. The bill in its current form, requires that a copy of personal data be stored within the Indian territory and certain critical personal data must be stored only within the country.[53] For processing of sensitive personal data, the bill requires that prior explicit consent of an individual be sought for processing.[54] It may be noted that while the bill provides this categorisation, the definitions are ambiguous and render the bill effectively a blanket data localisation measure. Imprecise definitions heighten the risk of excessive legislation.

Sectoral regulation of data has preceded the formulation of India's overarching privacy framework. The most prominent sector specific rules are RBI's notification on localisation of payment systems data that was implemented in haste. Recently, localisation was proposedin the Draft National E-Commerce Policy. In February 2019, a revised version was announced retaining localisation requirements. For example, the policy imposes restrictions on cross-border flow of data collected by IoT devices installed in public spaces, data generated by Indian users on Internet platforms such as e-commerce, social media, search, etc. It also tended to overextend to entities storing user data abroad prohibiting them to share their data with third parties, even with the user's consent. Recent developments indicate that data localisation norms would be kept out of the final e-commerce policy, thus leaving the matter to the discretion of the Ministry of Electronics and Information Technology (MeitY) to deal with in the Personal Data Protection Bill.

50. Bailey and Parsheera (2018)
51. Ibid;https://www.ikigailaw.com/data-localisation-requirements-for-telecom-and-internet-service-providers-current-law/#acceptLicense
52. "The Localisation Gambit". The Centre for Internet and Society (2019)
53. https://prsindia.org/billtrack/draft-personal-data-protection-bill-2018
54. Ibid

Figure 2.2 below provides a chronological presentation of the active and proposed measures of data regulation (including data localisation) in India. The extent of restrictions varies by sector. For example, while payments data has a local storage requirement, data under the e-Pharmacy regulations and critical personal data are completely prohibited from cross-border transfers with limited exceptions. The e-commerce policy allows cross border data flows, with mirroring, i.e., copy of the data should be stored within the country. The economic implications of these policies will naturally depend on several factors, including size of the entity, the business model and sector of operation. Please refer to Appendix 1 (Table A1.2) for a list of data regulations in India including details on the process of design and nature of localisation where applicable.

Figure 2.2: Active and Proposed Measures of Data Regulation in India



Source - Compiled by authors

The British economist Joan Robinson had once famously observed that "whatever you can rightly say about India, the opposite is also true". The passionate discourse around data localisation policies, both in favour and against, lends itself to that characterisation of India. But not with a negative feel. For an important subject such as data localisation, evidence will have to be collected, analysed and the options weighed before the policy in inscribed. Arguments in favour include enabling innovation, improving cyber security and privacy, enhancing national security and protection against foreign surveillance.[55] The white paper released by the Justice Sri Krishna Committee highlights that the development of an indigenous ecosystem of artificial intelligence can be a key driver of economic growth and that such innovation can be aided by storing data in India and granting Indian start-ups access to anonymised versions of the data.[56] Arguments against localisation include higher costs of doing business, faltering security systems, risks of retaliation and adverse impact on investments. Some Indian businesses, foreign businesses and foreign governments have spoken out against data localisation. For example,a note of caution was sounded that the RBI Directive on localisation of payments data could compromise fraud detection systemsand the detection of money laundering in the domestic payments system.[57] The Directive required payment companies to store data of Indian users exclusively on local servers and the deletion of back data from global servers.[58] The directive drew criticism from industry stakeholders for the lack of both, a due consultation process, as well as clarity on several aspects of compliance. This is discussed in further detail in chapter 4 of the report. Meanwhile RBI clarified that all payments data needs to be stored only in India, including end-to-end transaction details and information pertaining to payment or settlement transaction that is gathered/transmitted/processed as part of a payment message/instruction.[59]

The draft e-commerce policy has also been criticised. The Ministry of Electronics and Information Technology (MEITY) reportedly opposed the fact that the e-commerce policy attempted to prescribe rules on data management that was in many ways overlapping with the emerging data protection regime.[60] This issue was subsequently discussed with the Ministry of Commerce and Industry and sorted.

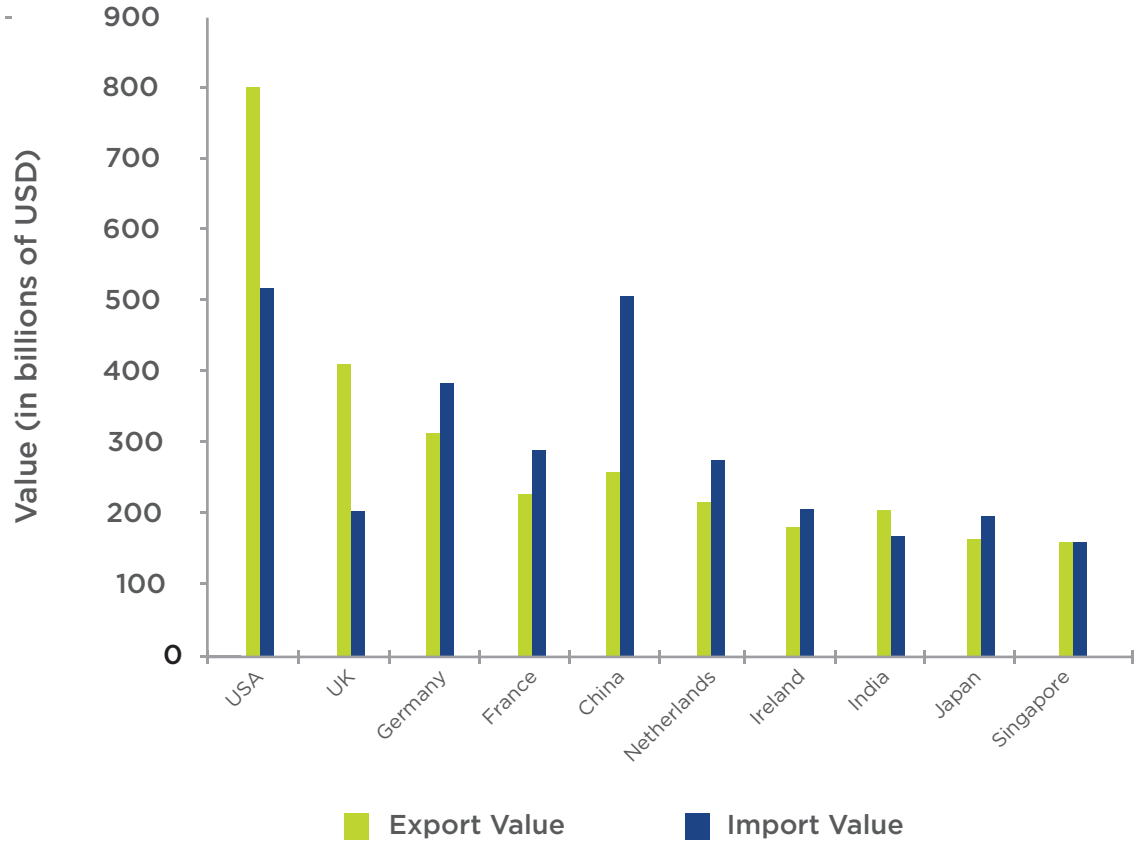
The 2019 National Trade Estimate Report on Foreign Trade Barriers by the US Trade Representative highlighted that India's data localisation requirements would act as a significant barrier to digital trade between India and the US.[61] Moreover, a policy that seeks to encourage domestic companies to build competitive advantage may end up hurting its own small and medium enterprises on account of localisation driven compliance costs.[62] The next three chapters delve deeper into some of these hypotheses and cull evidence from India on the economic implications of localisation measures using the international trade lens and costs to Indian and foreign companies operating in or engaging with India.

55. "The Localisation Gambit". The Centre for Internet and Society (2019)
56. White Paper of the Committee of Experts on a Data Protection Framework for India
57. https://www.livemint.com/companies/news/rbi-data-localisation-rule-may-compromise-fraud-detection-in-india-mastercard-1552889014479.html
58. https://www.livemint.com/Companies/MzB7AcmM9mOarQKh0BIn5J/Mastercard-will-delete-Indian-card holders-data-from-servers.html
59. https://www.thehindu.com/business/payments-data-must-be-saved-locally-rbi/article28159408.ece
60. https://tech.economictimes.indiatimes.com/news/internet/meity-miffed-at-ministries-sectoral-data-policies-ahead-of-privacy-law/68663254
61. https://www.livemint.com/industry/retail/us-criticises-india-s-data-localisation-norms-draft-e-commerce -policy-1554806134762.html
62. https://qz.com/india/1422014/rbis-data-localisation-could-hurt-indias-own-startups/

3. Impact of Cross- Border Data Flows on International Trade

Digital technology has become essential to the functioning of the global economy. It has not only transformed the way in which traditional industries function but has also changed the way economies, businesses, governments and institutions interact with each other. The modern Silk Route is characterised by undersea fiber optic cables and satellite links that carry electronic information.[63] Global delivery models are making it possible for workers to participate in foreign labour markets irrespective of immigration barriers. From being non-tradable, services today constitute a significant chunk of global economic activity. WTO predicts that the share of services in total trade will increase from 21 percent to 25 percent by 2030.[64] Figure 3.1 shows the value of services exports and imports for the top 10 countries in commercial services trade (2018).

Figure 3.1: Top 10 Countries for Commercial Services Trade in 2018



Source – WTO Press Release

63. Chander, Anupam. "Trade 2.0." Yale J. Int'l L. 34 (2009): 281.
64. World Trade Report – The future of world trade: how digital technologies are transforming global commerce (2018)

The impact of digital technologies is not limited to the expansion and facilitation of trade in services. It involves other sectors of the economy as well. For example, many goods such as books, music and movie CDs are consumed today in digital formats and known as digit is able goods. Digitalisation has led to a decline in the trade of these goods from 2.8 percent of total goods trade in 2000 to 0.8 percent in 2016, as estimated by the WTO. They have made geographical distances redundant and drastically reduced trade costs. Estimates show that international trade costs declined by 15 percent between 1996 and 2014 which could facilitate an annual increase of 1.8 percent to 2 percent in total trade until 2030, amounting to a cumulative growth of 31 percent to 34 percent over 15 years.[65] Digital trade has expanded product markets and product diversity and lowered concentration of export baskets.[66] The use of internet enabled devices and direct access to global e-commerce markets, has also reshaped consumer preferences. Figure 3.2 and 3.3 provide e-commerce revenue for select countries and the number of global e-commerce users over time, respectively.

Figure 3.2: E-Commerce Revenues of Selected Countries

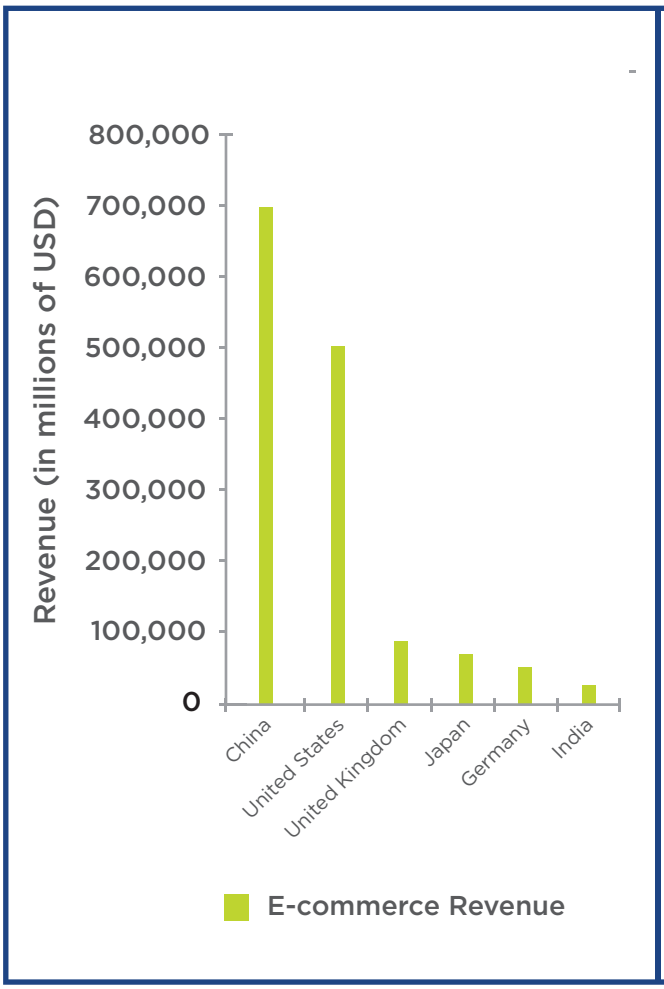
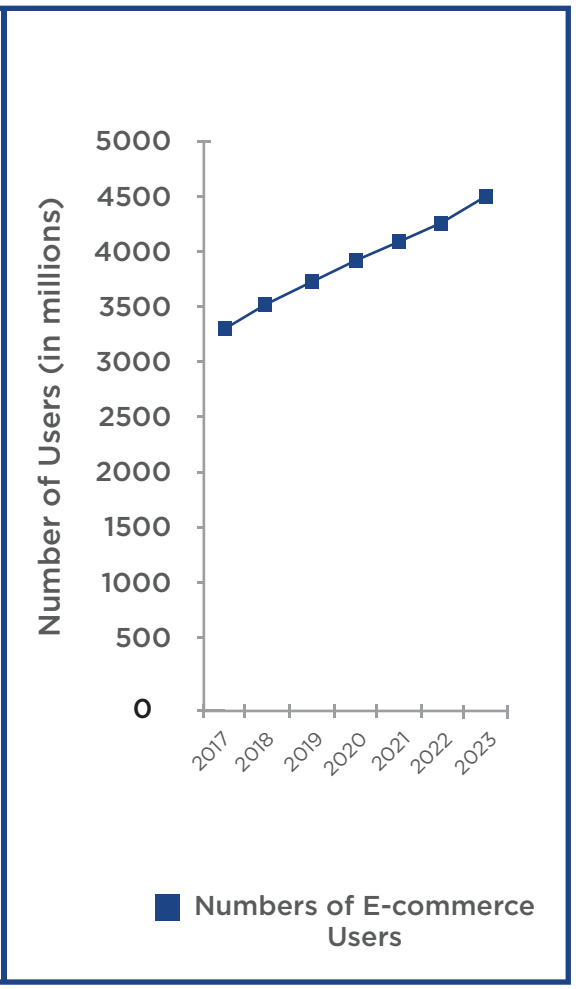


Figure 3.3: Global E-commerce Users



Source – Statista

65. Ibid
66. Ibid

E-commerce is found to have benefitted micro, small and medium enterprises (MSMEs) in developing countries[67]. Indigenous entrepreneurs and firms have found a way to reach their target customers by selling their products over the internet as well as by listing themselves on global online marketplaces. Small and medium sized enterprises that use internet-based business modelsare estimated to have a survival rate of 54 percent, which is 30 percent higher than that of offline businesses.[68] WTO estimates that the share of developing countries in global trade could increase from 46 percent in 2015 to 57 percent by 2030. Studies also show that e-commerce will result in an increase in the overall volume of trade. Moreover, countries that are open to imports from high income economies would benefit from knowledge spillovers and both direct and indirect job creation.[69]

The empirical literature evaluating the impact of information and communication technology on international trade is over a decade old. One of the first studies to consider this relationship was by Freund and Weinhold (2004) in which the authors used a sample of 56 developed and middle-income countries for the period 1995 – 1999. The number of website domain names in each country was used as a measure of internet availability. The study found that a 10 percent increase in the growth of internet led to a 1 percent increase in exports. Another study by Clark and Wallsten (2006) used a cross-section of 101 countries in 2001, to estimate the effect of the internet on export performance, controlling for levels of development. The study found that internet penetration was positively correlated with exports from developing countries to developed countries, but not to other developing countries. Thus internet connected firms in developing countries gain access to markets in the developed countries, where most enterprises are anyway connected to the internet. Data shows that over 90 percent of all young people use the internet, as compared to 67 percent in developed countries.[70] Latest data on internet penetration around the world shows that much of the growth in 2019 has been on account of developing countries.[71] Internet penetration in India has also grown at unprecedented rates in the last couple of years. Between 2018 and 2019, internet users in India increased by almost 100 million, demonstrating an annual growth of more than 20 percent.[72] With foreign trade in India increasingly geared towards a south-south exchange, we can establish correlation between increased internet usage and trade. However, unpicking the impact of the internet on India's trade with developing countries has to be econometrically tested.

Vemuri and Siddiqui (2009) used the gravity model to test whether ICT and the internet boosted international trade. The paper found that a 10 percent increase in internet adoption led to a 2 percent increase in bilateral trade. The authors concluded that ICT infrastructure and internet availability could be a policy instrument for boosting international trade and economic development. They concluded that speedy access to reliable information could be a significant factor in minimising risks inherent in international transactions. Appendix 2 (Table A2.1) summarises the methodologies and findings of some important studies in this context.

67. Pepper, Robert, John Garrity, and Connie LaSalle. "Cross-Border Data Flows, Digital Innovation, and Economic Growth." The Global Information Technology Report 2016: Innovating in the Digital Economy (2016): 39-40.
68. Ibid
69. Terzi, Nuray. "The impact of e-commerce on international trade and employment." Procedia-Social and Behavioral Sciences 24 (2011): 745-753.
70. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf
71. https://thenextweb.com/contributors/2019/01/30/digital-trends-2019-every-single-stat-you-need-to-know-about-the-internet/
72. Ciuriak and Ptashkina (2018)

3.1 Impacts of Cross Border Data Flows and Data Localisation

While traditionally trade liberalisation was based on four freedoms i.e. the free movement of goods, services, capital and persons, it is argued that a necessary fifth freedom is, the free movement of digital information.[73] ECIPE's Digital Trade Restrictiveness Index (2018)[74] ranks 64 countries on measures of digital trade. It covers a wide spectrum of digital trade policies that can be clustered into four large areas (i) fiscal restrictions and market access (ii) establishment restrictions (iii) restrictions on data and (iv) trading restrictions. The index shows that China is the most restricted country in digital trade, followed by Russia, India, Indonesia and Vietnam.

Digital and digitally enabled trade is dependent on access to the internet and the free flow of data across geographical boundaries.[75] A report by Business Roundtable identifies six different areas of business operations that entail transmission of data across borders. These are interconnected machinery, big data analytics, back-office consolidation, supply-chain automation, digital collaboration and cloud scalability.[76] As per a USITC estimate, the internet reduces trade costs by 26 percent on average.[77] Several traditional industries such as oil and gas, manufacturing and retail are also reliant on cross-border data flows for their routine decision making processes.[78] For example, Rio Tinto which is a world leader in mining and metals, operating in 40 countries across six continents, uses real time aggregated data to identify the size, location and quality of ore.[79]

According to an UNCTAD estimate, 50 percent of all traded services are enabled by technology and cross-border flow of data. A 2014 study by USITC finds that removing foreign digital trade barriers would increase US GDP by 0.1 - 0.3 percent and wages by 0.7 - 0.14 percent in digitally intensive sectors. The study also finds that digital trade raised GDP in the US by 3.4 - 4.8 percent and contributed to creating 2.4 million new jobs. McKinsey Global Institute (2016) estimates that data flows account for $2.8 trillion of total value generated in 2014.[80]

A study by Bauer et al. (2016) finds that data localisation and commonly used barriers to data flows decreased total factor productivity (TFP). This further reduced GDP by 0.1 percent in Brazil, 0.55 percent in China, 0.48 percent in the EU and 0.58 percent in South Korea. The Leviathan Security Group (2015) has also examined the cost of data localisation by comparing the cost of building data centres across countries. They find that local companies would be required to pay 30 - 60 percent more for their computing needs in the event of a forced data localisation legislation. The location choice for data centers are driven by considerations such as availability of infrastructure including power costs, suitable climate, political and regulatory environment, besides technical factors such as latency, data security, etc[81]. It is therefore no surprise that even within countries the location of data centers is concentrated in regions which provide a conducive environment. For example, in India, data centers have proliferated in the states of Telangana and Maharashtra. Organic growth of data centers it is argued, is more cost efficient than forced measures of localisation[82]. According to a study commissioned by the US Government, the average cost of setting up a data centrein Brazil is $60.9 million, in Chile, $51.2 million and in the U.S. it is $43 million and the corresponding operating costs (energy and other expenses) are on average $950,000, $710000 and $510,000 respectively.[83] Estimates from the Asia Pacific Data Centre Price Tracker shows that Japan has the largest data centre market among 7 countries in the Asia

73. Ibid
74. https://ecipe.org/dte/dte-report/
75. Op Cit, 72
76. Op Cit, 67
77. Ibid
78. Castro, Daniel, and Alan McQuinn. "Cross-border data flows enable growth in all industries." Information Technology and Innovation Foundation 2 (2015): 1-21.
79. Ibid
80. Manyika, J., S. Lund, J. Bughin, J. Woetzel, K. Stamenov, and D. Dhingra. "Digital Globalization: The New Era of Global Flows. New York: McKinsey Global Institute." (2016).
81. O'Connor, Brendan. "Quantifying the Cost of Forced Localization." Leviathan Security Group, June (2015).
82. Ibid
83. Loretta Chao & Paulo Trevisani, Brazil Legislators Bear Down on Internet Bill, Wall St. J. (Nov. 13, 2013, 6:45 PM ET), http://online.wsj.com/news/articles/SB10001424052702304868404579194290325348688
84. HongKong, Indonesia, Japan, Singapore, Malaysia, South Korea and Thailand

Data centre price levels also vary significantly across the region, with Indonesia having the lowest average rack space pricing (at USD $540 per month) and Hong Kong with an average rack space rate (at USD $976 per month). The highest average rack space rates in the region are found in Thailand (at USD $1,510 per month) and Singapore (at USD $1,414 per month) per rack.[85] Therefore, cost can be a primary driver determining the location of a data centre. Appendix 2 (Table A2.2) provides a detailed description of these studies, including a description of the methodology used and the findings.

3.2 The Model

Estimating the impact of data localisation for India, a country of subcontinental proportions, would be possible if sufficient sub-national data by sector and by state were available. In its absence, we estimate the impact of cross-border data flows on international trade at the level of the macro economy. India's gradual integration into the global economy since liberalisation has led to massive growth in foreign trade. In the last fiscal, India's overall exports were estimated to be US$ 535.45 billion, registering a 7.97 percent growth over the same period last year.[86] The ratio of total exports of goods and services to GDP has increased from 6.14 percent in 1990 to 18.78 percent in 2017.[87] Given the economic significance of foreign trade to India's growth, it is useful to identify its drivers. Using the previous discussion on the role of digitalisation in goods and services trade, we hypothesise that cross border data flows positively impact India's foreign trade. Towards this objective, we use an augmented gravity model of trade. The estimation is based ona panel data set of trade between India and 37 partner countries over the period 2014 to 2018.

The gravity equation was first applied by Tinbergen (1962) and Poyhonen (1963).[88] Studies have found that the gravity model of international trade explains as much as 75 percent of the variability in the levels of international trade.[89] The gravity model has its roots in Newton's law of force i.e. attractive force between two objects is directly proportional to the product of their masses and inversely proportional to the distance between them.[90] In the gravity model of trade, volume of bilateral trade between two countries is directly proportional to the product of the sizes of both economies, typically measured using their GDP, and inversely proportional to the geographical distance between them.

$$T_{ij} \propto GDP_i\ GDP_j/D_{ij}$$ [91]

where, T_{ij} the bilateral trade volume between countries i and j
GDP_i is the GDP of trading partner i
D_{ij} is the distance between countries i and j

Distance acts as a proxy for transportation costs and explains its importance and inclusion in a trade model.[92] However, Bougheas et al. (1999) showed that transport costs were not only a function of distance, but also of public infrastructure.[93] Since distance and income don't always explain the variability in trade, the traditional model was augmented, by introducing additional variables such as infrastructure determinants to explain the remaining variations. We adapt the augmented gravity model to build our model specification, that includes variables such as infrastructure, income differences and exchange rates as determinants of bilateral trade flows.

85. https://www.globenewswire.com/news-release/2019/01/30/1707414/0/en/Asia-Pacific-Data-Centre-Pricing-Tracker-2019.html
86. http://pib.nic.in/newsite/PrintRelease.aspx?relid=189768
87. https://data.worldbank.org/indicator/ne.exp.gnfs.zs
88. Martínez-Zarzoso, Inmaculada, and Felicitas Nowak-Lehmann. "Augmented gravity model: An empirical application to Mercosur-European Union trade flows." Journal of applied economics 6, no. 2 (2003): 291-316.
89. Vemuri and Siddiqui (2009)
90. Ibid
91. Ibid
92. Ibid
93. Op Cit, 88

We use the quantum of international internet bandwidth as a proxy for cross-border data flows. Available bandwidth reflects the capacity for cross-border flow of data; a consistent increase in bandwidth over time, can be safely assumed to reflect an increase in cross-border data flows. This data has been extracted from TeleGeography's Global Internet Geography database. In our data set of India's 37 trading partners, 14 countries do not share any internet bandwidth with India. In the absence of uniform bilateral data on services trade for India's trading partners, we use total goods trade as a proxy for total trade in our model. While services trade is more likely to be impacted by shared bandwidth, the increasing servicification of manufacturing and additive technologies such as 3D printing, along with the rise in mobile to mobile technologies and global e-commerce platforms, have made cross-border data flows equally important for merchandise trade. Total volume of bilateral trade in goods has been sourced from the UN Comtrade Database. The other determinants used in the specification are difference between per capita GDP of a trading pair, the real exchange rate between two countries and the geographical distance between a trading pair. The differences in per capita incomes have been computed using data from the World Economic Outlook (April 2019). Values for geographical distance have been obtained from the CEPII Gravity dataset. The data on exchange rates and GDP deflators is extracted from XE[94] and World Bank respectively. We take a logarithmic transformation of the explanatory variable for the purpose of estimation. Accordingly, the model is specified as follows:

$$X_{it} = \alpha + \beta 1\ logYPCdif_{it} + \beta 2\ logRER_{it} + \beta 3\ logIIB_{it} + \beta 4\ logDistance_{it} + \varepsilon$$

Where i refers to a trading pair and goes from 1 to 37
t refers to year t and goes from 2014 to 2018

The variables have been defined in Box 3.1 below.

Box 3.1: Definitions of Variables

$logX_{it}$ is the total volume of merchandise trade between India and a partner country in year t

$logYPCdif_{it}$ is the logarithmic value of the difference between the per capita incomes of India and partner country in a year t. Since we consider total volume of trade, the sign of the coefficient for per capita income differential can assume either a positive or a negative sign. From an exports point of view, a negative sign would be more intuitive. A positive sign implies that higher differences in per capita income, a proxy for differences in factor endowments, have a positive effect on exports. However, in this model, since we include total trade, a higher difference in per capita incomes explains the need for total trade, not with standing the identification of the origin and destination country.

$logRER_{it}$ is the logarithmic value of the real exchange rate of India, defined as the INR value of 1 unit of the partner country's currency, multiplied by the partner country's GDP deflator and divided by India's GDP deflator, in year t. The expected sign of the coefficient for this variable could be either positive or negative.

$logIIB_{it}$ is the logarithmic value of International Internet Bandwidth between India and its partner country. The expected sign of the coefficient of this variable would be positive as higher bandwidth is expected to positively affect overall volume of trade.

$logDistance_{it}$ is the logarithmic value of the geographical distance between India and its partner country. The expected sign of the coefficient would be negative, in accordance with the principle of the gravity model that volume of trade would be negatively related to geographical distance between two countries.

94. https://www.xe.com/currencytables/?from=INR

3.3 Estimation, Results and Interpretation

We use a dynamic panel data approach to estimate the model. The Arellano-Bond (AB) system estimator assumes that the necessary instruments in the model are internal, i.e., based on lagged values. This approach is most suited for a linear functional relationship and when the dependent variable depends on its own past realisations[95],[96].Our estimation produces significant and consistent results[97] confirming the stated hypothesis.

The results find

1 percent increase in international internet bandwidth leads to an increase of US$ 696.71 million in total volume of goods trade for India. From 2016-17 to 2017-18, total international internet bandwidth in India increased by 35 percent, thus leading to an increase of approximately US$ 24 billion in total volume of goods trade. During the same period, the absolute increase in India's total volume of trade was approximately US$ 202 billion. Therefore, approximately 12 percent of the growth in India's total volume of trade was on account of increase in international internet bandwidth.

The magnitude of the multiplier could be higher when bilateral services trade data is included in the model, as much of the trade in services, Mode 1 services in particular, is facilitated by the internet.

Between 2014 and 2018, the compounded annual growth rate (CAGR) of international internet bandwidth was 63 percent. At the projected rate of growth of international internet bandwidth, India's total volume of goods trade could increase by US$ 43 billion annually, on account of increase in internet bandwidth.

Coefficients for other explanatory variables in the model are also significant. The difference in per capita income between India and its trading partners (denoted by the variable $logYPCdif_{it}$) and the real effective exchange rate (denoted by the variable $logRER_{it}$) have positive coefficients, while that for distance is negative. The results reinforce existing empirical evidence. Refer Appendix 3 for a summary of the results.

The model presents an estimate of the impact of cross-border data flows on India's volume of trade. The model calculates an unambiguous positive relation between internet bandwidth and volume of trade. Since internet bandwidth is used as a proxy for cross border data flows, the implication of the result is that any constraint on cross border data flows will disproportionately impact volume of trade. In other words, a 1 percent decline in cross border data flows will reduce the volume of trade by US$ 696.71 million. The precise impacts will of course be established once the nature and volume of restrictions are known within each sector. As a practical matter, not all cross-border data flows are personal or sensitive, the categories that will potentially be impacted by localisation measures. But policy often has impacts that spillover to other categories, sometimes inadvertent. The next two chapters will explain the macro-economic result by illustrating business processes that are likely to get impacted. The detailed discussions on changes in data processing and data storage practices will complement the results presented in this chapter.

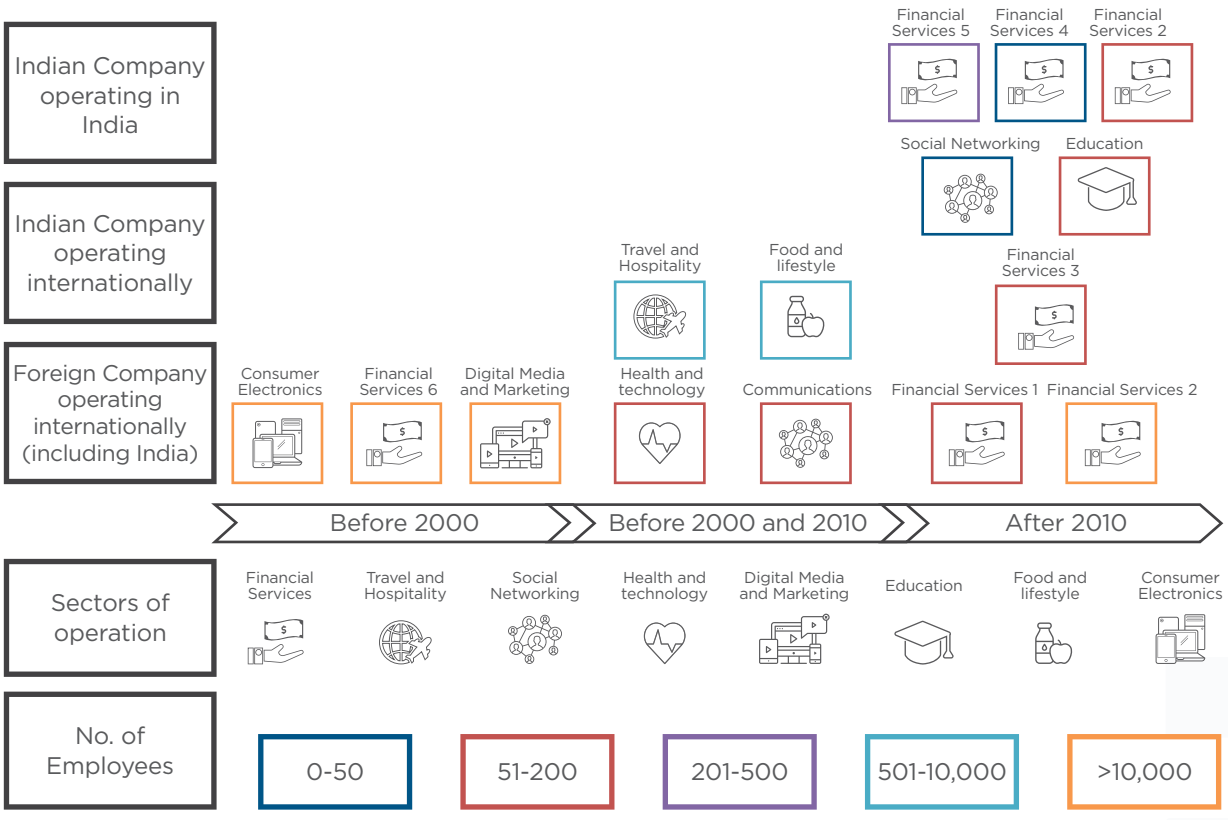
95. http://fmwww.bc.edu/EC-C/S2013/823/EC823.S2013.nn05.slides.pdf
96. In our specification the total volume of trade in period t between India and its partner country is likely to depend on the volume of trade in period t-1. Also, right-hand side variables (explanatory variables) may not be strictly exogenous; the quantum of international internet bandwidth may be endogenous to the level of trade between India and a trading partner. The AB estimator sets up generalized method of moments in which the model is specified as a system of equations, one per time period, and the instruments vary with each equation
97. We use robust standard errors to check for heterogeneity. We also plot the residuals with the estimated values for total trade to check omitted variable bias. All tests hold to establish to robustness of the model.

4. Case-Study Analysis

Chapter 3 does not capture the dynamic through which impacts of data localisation policies are likely to manifest across sectors and business types. Evidence has shown that the costs of data localisation are likely to be the highest for sectors such as communications and financial services.[98] The financial services industry in India is currently a mix of local and global players; their globalised service delivery models are therefore susceptible to localisation mandates. For example, it could impact the ability of financial services companies to share data across third-party operators on credit history, transaction data, etc. that helps identify frauds and coordinate remedial actions.[99] This chapter, while considering view-points of companies across various sectors, brings focus to the financial services sector that is generating enormous amount of data, that is largely personal in nature. Moreover, this is the most recent policy that helps build some evidence on the costs and benefits of data localisation. The other policies discussed in Chapter 2 are still proposals.

The analysis in this chapter is based on fifteen in-depth case studies that utilise internet-based delivery models, some more, some relatively less, but all generate data as part of their business process. Names have been masked to respect confidentiality. Our sample consists of three categories of companies – companies of Indian origin operating internationally, companies of Indian origin operating exclusively in India and companies of foreign origin operating internationally including India. The case studies help understand the principal business models, data management processes, quantum of cross-border data flows and the impact that different types of data localisation might have on the efficiency and profitability of these businesses. The companies vary in size and age. The sample includes 2-year-old startups with 10 employees on one extreme and decade old companies with over 10,000 employees on the other. Figure 4.1 illustrates the variety in the sample. The categorisation by sector is based on their original or primary functionality, although several of these companies have now diversified into multtiple services.

Figure 4.1: Framework for Selection of Case Studies



Source – Compiled by authors

98. Bailey and Parsheera (2018)
99. https://thewire.in/business/rbi-payment-data-localisation-india

Based on the inputs provided by different stakeholders, we divide the discussion into three sub-sections (i) variations in data management processes across companies and sectors. (ii) impact of restrictions on cross-border flow of data and (iii) policy concerns raised by businesses. Details related to each company are provided in Appendix 4.

4.1 Data Management Processes

Data management is understood to be an administrative process that involves acquiring, validating, storing, protecting and processing data, is a core business activity for all fifteen companies. Most enterprises use external cloud networks to store data; only a handful of companies in the sample maintained their own data servers. None of the companies reported using a hybrid model i.e. part cloud and part own data centres, for data storage. For startups with tight cash flows, cloud computing provided the much-needed access to resources without large capital expenditures.

There are two primary observations relating to data storage evident from our interaction. There is a pattern of migration from managed data servers to leased cloud services, and migration from cloud services located on foreign soil to cloud services in India. The former trend is on account of the agility and ease of scalability provided by cloud services while the latter is in anticipation of localisation requirements likely to emerge in the future. A travel and hospitality company of Indian origin reported that rapid scaling up of services created maintenance challenges of owned data centres. Hosting data on cloud allowed for need-based expenditure, as opposed to significant investments in maintaining captive data centres.

In anticipation of a data localisation requirement that may arise in the future, startups in particular have moved their data to cloud services in India. Since startups are typically dependent on external funding and have tight cash flows, additional costs of regulatory compliance can become burdensome. A communications app of foreign origin with one of the largest markets in India reported having two data centres – one in India and one in Europe. Their data is classified into EU and non-EU data. Data pertaining to EU customers is stored in the EU, while all data pertaining to customers outside the EU is stored in India. Similarly, a US based social enterprise, working on health and technology related development projects for the government of India, was required to store their data on National Informatics Centre (NIC) servers in India. This data was later moved to a private cloud service provider in India for better efficiency. However, the company continues to maintain a server in the US.

Data management for companies in the financial services sector is particularly complex. The nature and volume of data collected by financial services companies exposes them to additional compliance requirements, especially with respect to policies on sensitive and personally identifiable data. By their very nature, financial services are closely monitored and any changes in the policy on data management can significantly impact costs. One financial services company of Indian origin operating exclusively in India stored data on a cloud in Singapore. However, RBI's local data storage directive in April 2018 prompted migration of their data from Singapore to a data centre in Mumbai. The company also reported that it segregates sensitive information of users from the overall data collected and stores it separately. This data is stored in an encrypted form, following industry encryption standards. Another small-sized and relatively new company of Indian origin offering financial services and operating in a few countries other than India used personally identifiable data for operational purposes, which was purged immediately after use. This meant that the company did not store any of the data it used and is therefore not likely to be impacted by localisation requirements in India, at least with respect to the current proposal of the Personal Data Protection Bill. A big sized consumer electronics company offering payment solutions reported that transaction details including personally identifiable or sensitive data were stored by third party banks or card companies. Therefore, there was currently no anticipated impact of the proposed data localisation regulations on this company. Smaller NBFCs operating solely in India reportedly found it easier to comply with localisation requirements.

During the period 2014 to 2018, the number of functional data centres in India increased from 27 to 33. While the number of data centres in India are very small compared to those in China and United States, they do indicate a rising trend. Forecast suggests that the Indian data centre market is expected to reach a value of USD 4 billion by 2024, with a CAGR of 9 percent between 2018 and 2024.[100] According to a report by NASSCOM, mushrooming of startups with internet-based delivery models, and the growing adoption of big data analytics and artificial intelligence is likely to enable a three-fold growth in India's cloud market to USD 7.1 billion by 2022. The growth in India's overall IT infrastructure is predominantly driven by a shift from 'cloud first' to 'cloud only' models, particularly for startups. Policies towards data localisation therefore need to recognise the emerging ecosystem so as to balance the need for data integrity with India's growing forte in the data economy. Several companies interviewed as a part of the study reported storing their data in India in anticipation of localistaion requirements, but at increased costs. For example, an Indian startup operating in multiple countries stated that the overall package of services including price, provided by Indian cloud service providers, or even newly established data centres in India by global players, were inferior to their foreign counterparts. A food and lifestyle company of Indian origin, reported storing data in a cloud network in Singapore, where they could avail a larger number of services compared to the cloud network in India, belonging to the same service provider. This may change in the future. With foreign players such as Amazon and Google opening data centres and cloud regions in India, the services will improve. At the moment, complexity associated with global business models, especially for companies operating in multiple countries will make compliance with localisation requirements hard and costly. The opportunity costs of data localisation are discussed in the next sub-section.

4.2 Opportunity Costs of Data Localisation

The impact of data localisation is found to be different between companies within the same sector as well as across sectors. Size of the company, matters. Most small and medium sized enterprises of Indian origin operating exclusively in India, reported a one-time cost of migration and no recurrent impact from localisation. In the short to medium run, however, these companies might have to contend with the existing quality of service available at data centres in India. With several global service providers scaling up services in India, local data centres will eventually match up to their overseas counterparts. A small sized financial services company of foreign origin, operating in India, revealed a preference for storing data outside India had there not been any localisation requirements. A social enterprise working on Government of India projects, noted that the government's first priority was to ensure that all information related to social welfare schemes and initiatives be stored in India, even if it meant delay in the implementation of projects. This is an example of the opportunity cost of data localisation, and one which the government is willing to internalise. On the other hand, there could be other unknown and unanticipated costs that strict data localistaion policies could produce, damaging some of India's comparative advantage in the space.

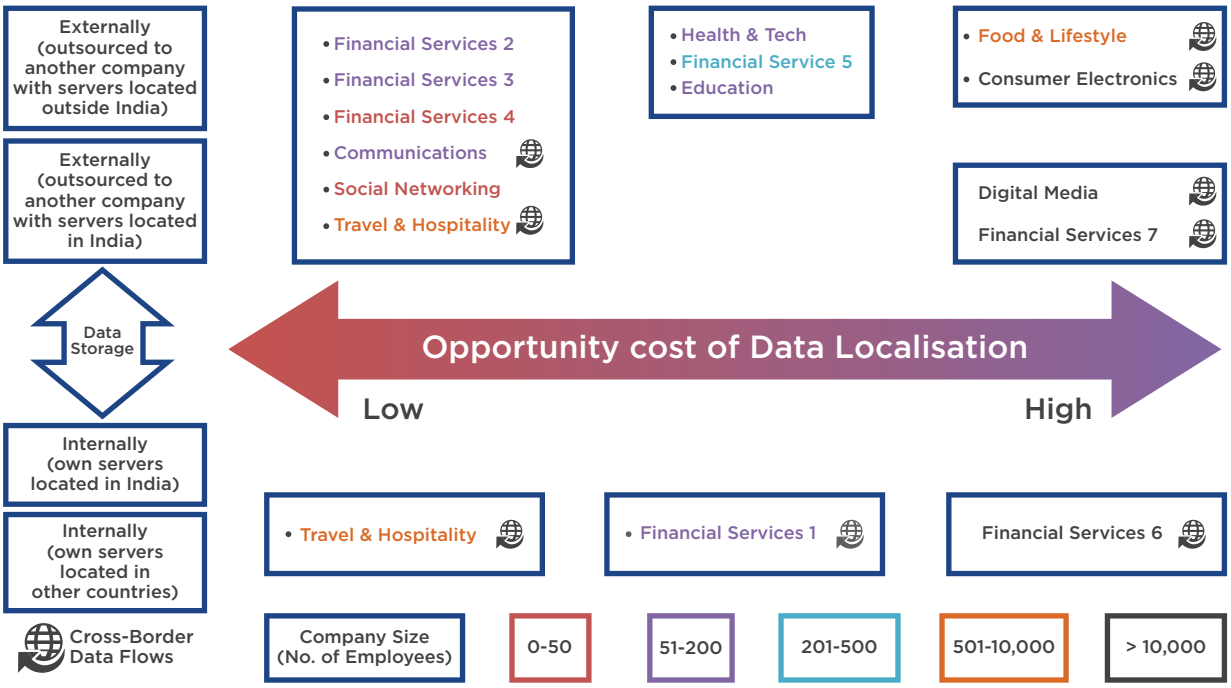
The most significant impacts of localisation were reported by a mature financial services company of foreign origin operating worldwide, a consumer electronics company of foreign origin operating worldwide, a payments (financial services) company of foreign origin operating internationally and a digital media and marketing company of foreign origin operating worldwide. The digital media company noted that increased costs could be potentially passed on to consumers. Figure 4.2 captures the relative opportunity cost of data localisation for the companies considered in this analysis. These costs include those that have been absorbed by the firm or those likely to be incurred in the future. In some cases, companies currently complying with localisation have expressed a preference to locate their data outside the country for improved business efficiency. The vertical axis in Figure 4.2 separates companies on the basis of their data storage practice. Companies which engage in cross-border data flows may or may not store their data in India. For those who store their data in India, the impact is relatively low. However, companies which currently comply with localisation norms but do not engage in cross-border data flows, also indicated a preference for locating data outside India, reflecting moderate opportunity costs of localisation. Companies with localised businesses reported no impact from localisation. One particular domestic company claimed that localisation improves their competitive advantage vis-à-vis foreign operators.

100. http://bwcio.businessworld.in/article/India-Data-Center-Market-2019-2024/06-02-2019-166872/

A primary point of contention for global financial services companies was the requirement to store user data for Indians exclusively within its jurisdiction without any copy of it being maintained in global servers. This implies that data of Indian citizens would have to be erased from global servers. Such a requirement seems unique to India, even across countries that impose some form of localisation. Most mature financial services companies use integrated global architectures for data management. Data localisation is likely to impair their fraud detection and anti-money laundering systems. These companies established operations in India under a system of unrestricted cross-border data flows. However, post the RBI directive (2018), compliance meant a structural change in their operating system. One stakeholder, for example, suggested that the benefits of global specialised databases to trace fraud and minimise fraud losses would be adversely affected by localisation. Erasing data of Indian citizens from global databases and having a separate ecosystem for India, according to them, would cut off Indian customers from the updates and innovations in the global system. Replicating the same changes in the Indian system would not only be expensive, but would be time lagged as well. Moreover, the cost of compliance is not likely to be one-time. The costs of maintaining and upgrading these systems, unique to each company, would be recurrent and significant. Financial services companies in our sample also reported the possibility of sub-optimal server capacities in India impacting their overall efficiency.

The food and lifestyle company of Indian origin uses cloud services hosted in Singapore. They worry about the quality and costs of data services in India if they are forced to migrate. While it may be difficult for them to pass on these costs to consumers in a hyper competitive digital services market, business partners are likely to bear the brunt of this increased cost.

Figure 4.2: Opportunity Cost of Data Localisation



Source – Compiled by authors

Among the policy objectives driving data localisation is the realisation of India's economic interests including the growth of India's indigenous data ecosystem. An argument favouring data localisation is the expectation for it to boost data storage infrastructure, build data analytics capabilities and generate more jobs. Some companies reported that forced development of data centers is likely to increase costs for businesses, as the cost of other supporting infrastructure such as power was significantly higher in India. Moreover, since data centers mostly run on auto-pilot and access to the systems are well-guarded, the operations are virtual with only a handful employed directly. A project concept on the establishment of data centres in Gujarat, indicated the manpower requirement for a data centre at Gandhinagar with 1080 racks to be the sum total of 12.[101] Some companies believed that data localisation would lead to better latency if servers are located in India, even if it meant higher costs. On the other hand,SMEs operating in the fast growing SaaS segment with clients primarily in the US, found storing data in a US data centre, more efficient, both in terms of costs and latency.[102]

A binary discourse on data localisation appears impossible. The need to promote data centers in India and domestic entrepreneurs needs to be seen in the context of the opportunity costs of forced localisation. Is the market-based approach in which businesses choose to locate servers in India more efficient than a government mandate? A global financial services company points out that SMEs across the world are coming up with innovative business models. Data localisation would deter such innovations and might prove counterproductive to the objectives of innovation and competition.

4.3 Policy Preferences

The effectiveness of a data localisation mandate is still subject to debate. A recurrent view across stakeholder interviews is the irrelevance of location of data to improving privacy outcomes. The oft quoted example is EU's GDPR that supports privacy without the need for local storage. At the same time, it is a trade barrier with implications for efficiency. Data localisation would entail additional compliance costs for several companies. Moreover, for those that want to enter the Indian market, increased costs of data localisation might act as an entry barrier. This is true particularly for foreign SMEs and startups. While large foreign firms are able to absorb the compliance costs in order to maintain access in India, foreign SMEs that are typically innovation intensive, might be crowded out. Finally, some felt there exists the risk of retaliation against India's localisation measures. Such measures can adversely impact India's domestic firms which rely on global markets. For example, big Indian IT companies that rely largely on off-shore models using citizen data of other countries, are likely to be impacted should countries retaliate to India's localisation measure.

Given their interest in India's billion plus market, foreign financial entities are prepared to comply with RBIs localisation directive. However, lack of clarity on compliance requirements makes compliance difficult. This is also true of the draft Personal Data Protection Bill, 2018 that fails to provide clarifications on the classification of data. Soft measures of data localisation such as mirroring of critical personal data were offered as alternatives to hard data localisation that prohibits any cross-border flow of data. The costs of mirroring would depend on the frequency with which data in the original location gets changed or updated. Secondly, data adequacy and data sharing arrangements with different countries was also a suggested alternative. A payments company suggested that providing a regular data dump to country regulators to help law enforcement requirements, could be an alternative to a hard data localisation measure. The policies in India were also criticised on grounds of over reach. For example, the use of "unfettered supervisory access" in RBI's directive leaves a lot of flexibility for regulators to take action against companies. Moreover, there is significant overlap in the application of different policies. The data collected by payments companies are already stored by third party banks which are duly regulated by the RBI. In effect, this data is already available with the government.

Finally, companies suggested that building a domestic digital ecosystem is not completely dependent on local storage of data. Complementary developments in quality of infrastructure, investments in intellectual capital including data analytics are equally necessary to satisfy this objective. The key findings from the case study analysis are summarized in Box 4.1

101. http://www.indextb.com/documents/Data-Center.pdf
102. These are insights from a forthcoming study by ICRIER on the regulatory impact of data localisation on MSMEs.

Box 4.1: Summary of Findings from the Case Study Analysis

I. Data Regulations and the Emerging Data Storage Ecosystem in India

- There is a pattern of migration from managed data servers to leased cloud services, and migration from cloud services located on foreign soil to cloud services in India. The former trend is on account of the agility and ease of scalability provided by cloud services while the latter is in anticipation of localisation requirements likely to emerge in the future.
- While India may not have been a natural choice for most companies to store and process data, many companies interviewed as a part of the study reported storing their data in India as a pre-emptive measure for policies likely to be introduced in the future.
- The services of foreign cloud operators have scaled manifold in India. Indian cloud service providers, however, continue to lag behind global service providers such as Amazon, Google, Microsoft etc. both in terms of quality and availability of sophisticated features as well as cost effectiveness. The growth in domestic IT infrastructure is being organically driven by India's push for IoT systems, the mushrooming of startups with internet-based delivery models and the growing adoption of big data analytics and artificial intelligence.
- Data management for companies in the financial services sector is particularly complex. The nature and volume of data collected by financial services companies expose them to additional compliance requirements, especially with respect to policies on sensitive and personally identifiable data.

II. Data Localisation – Implications on Cost, Innovation and Privacy

- Since most mature financial services companies use integrated global architectures for data management, localisation is likely to impair their fraud detection and anti-money laundering systems. The fraud detection systems could be weakened leading to a ten-fold increase in fraud losses in India. Moreover, the cost of compliance is not likely to be one-time. The costs of maintaining and upgrading these systems, unique to each company, will be recurrent and significant.
- A food and lifestyle company of Indian origin currently using cloud services hosted in Singapore feared that the applications provided by their existing cloud service provider may not be all available at the same cost in India. While it may be difficult for them to pass on these costs to consumers in a hyper competitive digital services market, business partners are likely to bear the brunt of this increased cost.
- Most small and medium sized enterprises of Indian origin operating exclusively in India, reported a one-time cost of migration to local data centers, if at all, and no ongoing impact from localisation. In the short to medium run, these companies might have to suffer from the lack of adequate features available in the Indian data centres.
- Several companies reported that forced development of data centers is likely to increase costs for businesses, as the cost of other supporting infrastructure such as power is significantly higher in India.
- Despite incurring moderate costs, some companies were of the belief that data localisation would lead to lesser latency if servers were located in India.
- While data localisation might lead to a competitive advantage for domestic companies in the short run, vis-à-vis their foreign competitors; in the long run, such an entry barrier might prove detrimental as innovation would be thwarted and the market will become less competitive.
- For companies that want to enter the Indian market, increased costs of localisation might act as an entry barrier. This is particularly true for foreign SMEs and startups for whom this cost might be significant.

- Most stakeholders agreed that the location of data is inconsequential to improving privacy outcomes.
- Companies also feared global retaliation against India's localisation measures. Such measures can adversely impact India's domestic firms, such as Indian IT companies which rely on global markets.

III. Policy Perspectives

- The perceived benefits, such as growth of the data economy and indirect job creation, accruing from data localisation can be achieved through alternate means that are less disruptive for global businesses
- The lack of clarity on guidelines make it difficult for firms to prepare for compliance with localisation norms, as pointed out by stakeholders with respect to RBI's 2018 Directive. The draft Personal Data Protection Bill in its current form is also vague about the classification of data. Such ambiguities increase compliance costs and must be addressed.
- In order to meet government objectives mid-way, several alternatives to localisation were proposed by the companies. Data mirroring and exchange through bilateral and plurilateral mechanisms were proposed as alternatives to hard localisation.

5. Insights from a Survey of Enterprises in India

In the previous chapter, we collected and analysed detailed information of fifteen companies whose operations are largely internet enabled. With digitalization becoming pervasive we expect traditional industries to also be affected by restrictions on cross-border data flows.[103] Thus to widen the ambit of the research and to enrich our analysis, we conducted a survey of business enterprises drawn from the traditional manufacturing and services sector, in addition to typical examples from the digital economy.

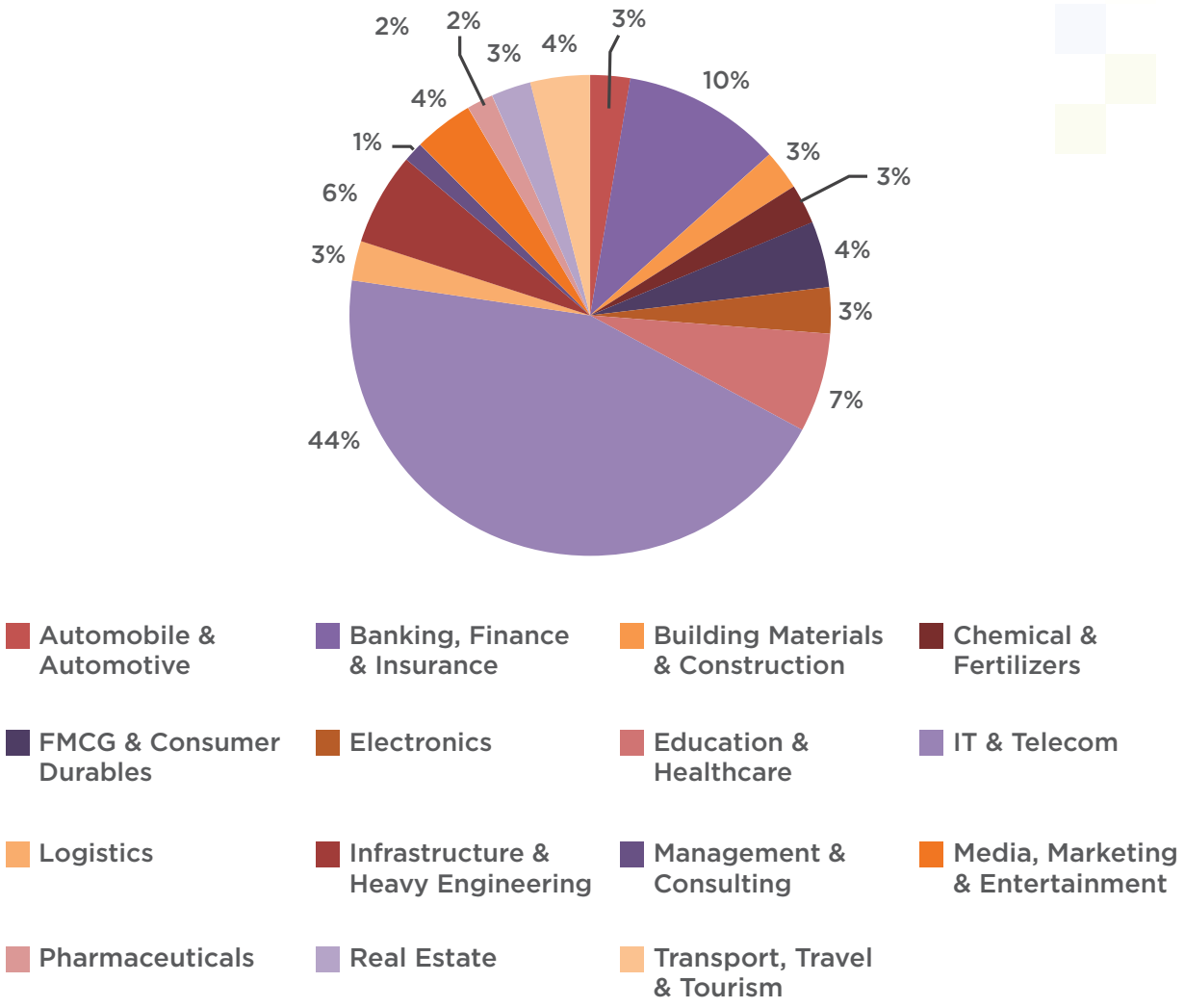
The survey analysis captures company views on data management processes, importance of cross-border data flows and impact or potential impact of data localisation, if any. Please refer to Appendix 6 for a copy of the questionnaire. Before the final roll out of the survey, several pilots were conducted to help finalise the questionnaire.The data was collected over a period of two months. In order to maintain confidentiality, the data collection followed a double-blind policy to encourage participation from foreign firms. However, the process met with limited success. The sampling failed to elicit responses from a wide range of foreign firms operating in India or waiting to invest in India. However, it provides a comparison between firms representing broader industry categories vis-à-vis those belonging to the category of internet-based business models. The results of the survey are best understood as an attempt to showcase the wide ranging impacts both in terms of processes impacted and its magnitude, as perceived by different types of firms.

5.1 Sample Description

Our sample consists of 225 business enterprises spanning across sectors like IT & Telecom, Infrastructure & Heavy Engineering, Logistics, Pharmaceuticals etc. Figure 5.1 shows the sector wise distribution of the sample. IT& Telecom is represented by 44 percent of the sample, followed by Banking, Finance & Insurance with a 10 percent share. All firms are located in one of 6 major metropolitan cities in India – Bangalore (22 percent), Chennai (13 percent), Delhi (33 percent), Hyderabad (9 percent), Kolkata (20 percent) and Mumbai (3 percent).[104]

103. Castro and McQuinn (2015)
104. Values in parentheses denote the percentage of firms in the sample that belong to a city.

Figure 5.1: Sector-wise Distribution of Sample



Most firms in the sample are private sector enterprises[105]. The data set also includes several multinational corporations, of which about half are headquartered in India and the other half in countries such as US, UK, Belgium, Egypt, Netherlands, New Zealand, Spain, etc. Not just group companies alone, several other companies also reported the presence of offices outside India. The sample includes enterprises that spread across micro, small, medium and large firms. The smallest firm hires three employees, while the largest firm employs 11,000 employees at location of interview (not including other offices). The median employee strength for the enterprises surveyed is 200.

5.2 Data Management and Data Processing

Feedback on data use and data management included responses to data storage preferences, storage capacity, uses of data, cross-border flow of data, data segregation, etc. The results vary widely across firms in the sample. 57 percent of the sample categorised data management to be a supporting business activity, while 40 percent categorised it as a core business activity. Firms which report data management as a core business activity belong to IT & telecom, logistics, infrastructure & heavy engineering, consumer goods and pharmaceuticals.

105. There are three public sector firms which are already mandated to store data in India and therefore not impacted by any new policy on localisation.

As volumes increase, server capacity in India is a limitation, both in terms of its ability to process as well store data. We find that firms on average leased 1600 terrabytes of storage capacity and operated at about 60 percent of that capacity. The sample includes data intensive firms in the IT & Telecom, infrastructure and heavy engineering and transport services that stored tens of thousands of terrabytes of data. Firms using data as a core business activity maintain a marginally higher buffer in terms of spare capacity.

In the sample, 60 percent firms reported storing data in a single location, in one of the four options, i.e., either on their own servers located in India or in another country, or in outsourced servers located in India or in another country. The remaining firms stored data in more than one location, up to four different options. Refer to Appendix 5 for details on the combinations of location preferences for data as reported by firms. Figure 5.2 shows the distribution of firms using a single location. Of the 60 percent firms that store data in a single location, 89 percent have in-house data storage infrastructure located in India. A few firms stored their data on their own servers that are located outside India. None of the firms using a single location opt for external data storage facilities outside India. For firms storing their data in two locations, five reported their data headquarters to be outside India. These firms belong to the IT & telecom and banking, finance & insurance sectors. Firms choosing to store data in multiple locations and formats, was an observable trend even in the small set of companies selected for the case study analysis.

Figure 5.2: Distribution of Firms by Location of Data which use a Single Location

About 102 firms, i.e. 45 percent of the firms in our sample, reported that their business involved cross border flow of data, especially with Singapore, Malaysia, UK and the US. Of these, 80 firms i.e. 78 percent of 102 firms reported that up to 30 percent of their total data moves across borders. However, three firms, an IT firm, a logistics and an airlines company each reported that more than 50 percent of their total data moves across borders. Refer to figures 5.3A and 5.3B for a distribution of these 102 firms by the share of cross border data in their total data and the share of personal data in cross border data, respectively. Boeing is an eminent example of a company using global data to reduce flight delays and cancellations.[106] For logistics companies 'electronic wrappers' that track goods through ports and depots, from source to destination, are also supported by cross-border data flows.[107] The integrated international supply chain based on cross-border data flows eventually benefits consumers with higher efficiency and lower prices.[108]

106. See Castro, Daniel, and Alan McQuinn. "Cross-border data flows enable growth in all industries." Information Technology and Innovation Foundation 2 (2015): 1-21
107. "Cross-Border Data Flows, Realising benefits and removing barriers". GSMA (2018)
108. Ibid

From a data localisation perspective that largely deals with restrictions on flows of personal data, and in some cases non-personal data, most firms reported that personal data comprised less than 10 percent of their overall cross-border data flows. Our sample consists of firms that are involved in low to moderate cross border personal data flows. Sectors such as automobiles, auto components, chemicals and heavy engineering fall within the category of low personal data flows while firms belonging to IT and telecoms belong to themoderate category.

Figure 5.3:

A: Distribution of Firms by Data Flows across Borders

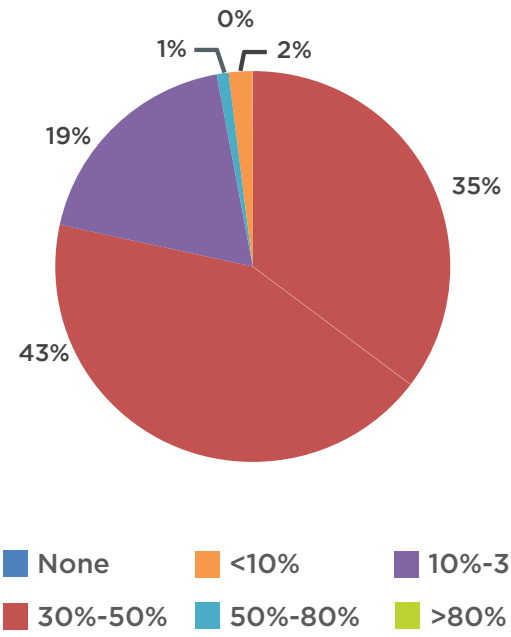
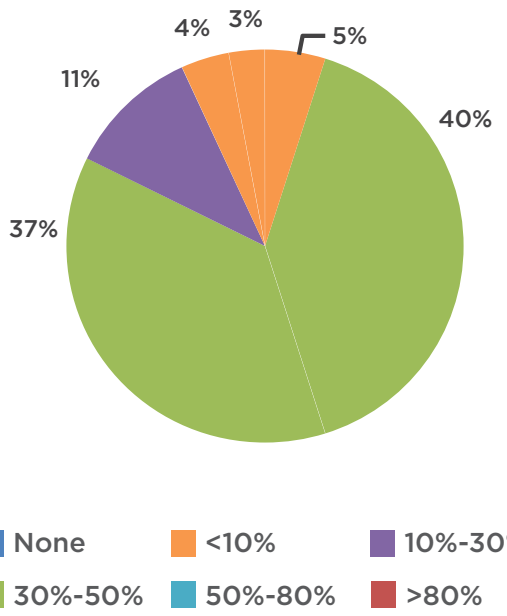


Figure 5.3:

B: Distribution of Firms by Share of Personal Data in Cross-Border Data Flows



Data management costs for the sample firms is around 1% of the total cost on average with firms in IT and logistics reporting higher management data costs. Figures 5.4 illustrates the distribution. Firms storing data on outsourced platforms incurred lower data management costs on average.

Figure 5.4:
A: Distribution of Firms by ICT Costs

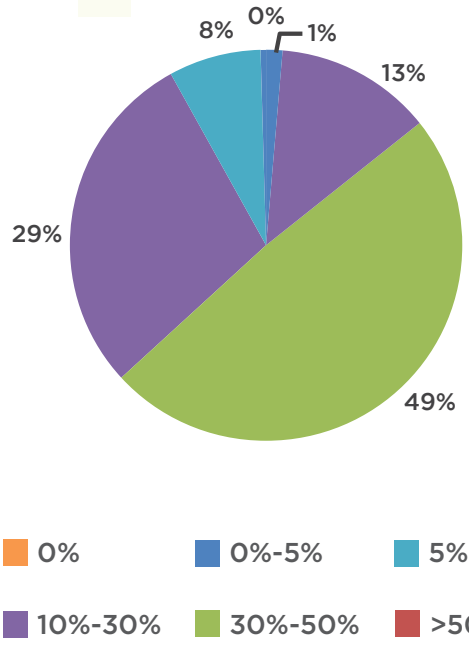
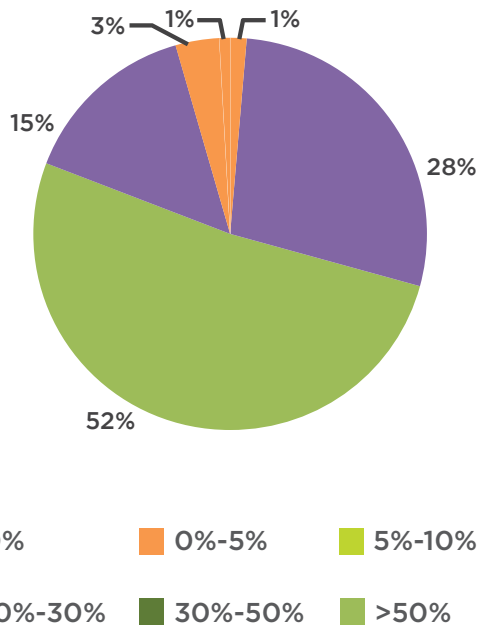


Figure 5.4:
B: Distribution of Firms by Data Management Costs in Overall ICT Costs



5.3 Impact of Data Localisation

In order to calibrate the impact on localisation we use three different scenarios – (i) Regulations that demand local storage of data but do not restrict cross -border data flows (ii) Regulations that demand local storage of data but restrict transfer to only a few countries (iii) Regulations that demand local storage of data and completely ban cross-border flow of data.

Given the data localization is a new policy, enterprises expressed inability to estimate precise costs. Of the 225 enterprises, 186 provided an estimate of the impact, but largely speculative in nature. Of the firms reporting an impact, the increase in ICT and data management costs is in the range of 10 percent. Other firms reported no impact while some reported a decline. Some local firms operating only in domestic market and storing the data locally reported an improvement in competitiveness due to data localisation. This needs to be, however juxtaposed with the fact that improvement in competitiveness is based on localisation raising the foreign firms cost of doing business rather than the domestic firm improving in its own efficiency. Evidently, domestic firms perceive data localisation as an opportunity that drives up costs for foreign business, giving them an opportunity in the short run to gain market share. There is another cohort of 100 firms that reported an increase in cost to downstream businesses / consumers as a consequence of localisation. A large number of these firms are headquartered in India. While foreign firms operating in India will unambiguously be impacted by localisation, some domestic firms are also likely to face cost disadvantages.

The firms that estimated lower costs, is on account of cheaper cloud services in India, though of poorer quality and lower technical efficiency. In the third scenario of a blanket localisation policy, some firms have responded with higher levels of impact, especially for group companies with offices both inside and outside India. Figures 5.6 and 5.7 provide the number of firms on the basis of the impact of data localisation on ICT and data management costs respectively.

Figure 5.5: Impact on ICT Costs if Proposed Data Localisation Measures are Implemented

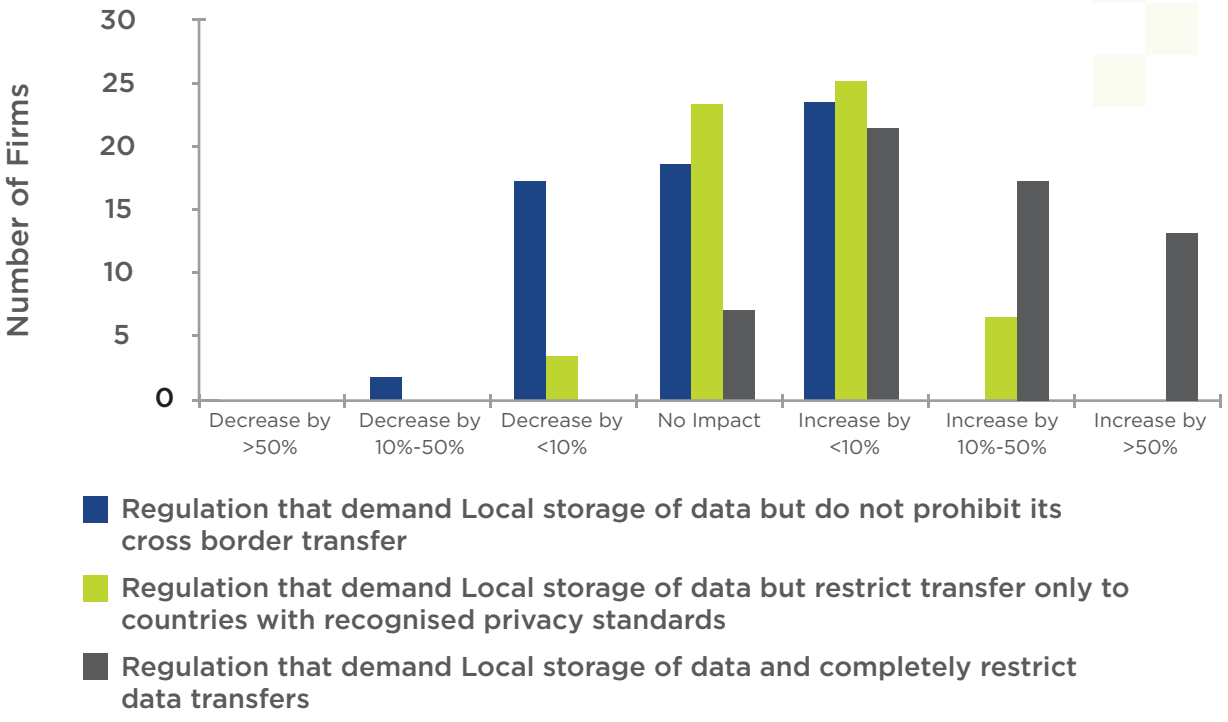
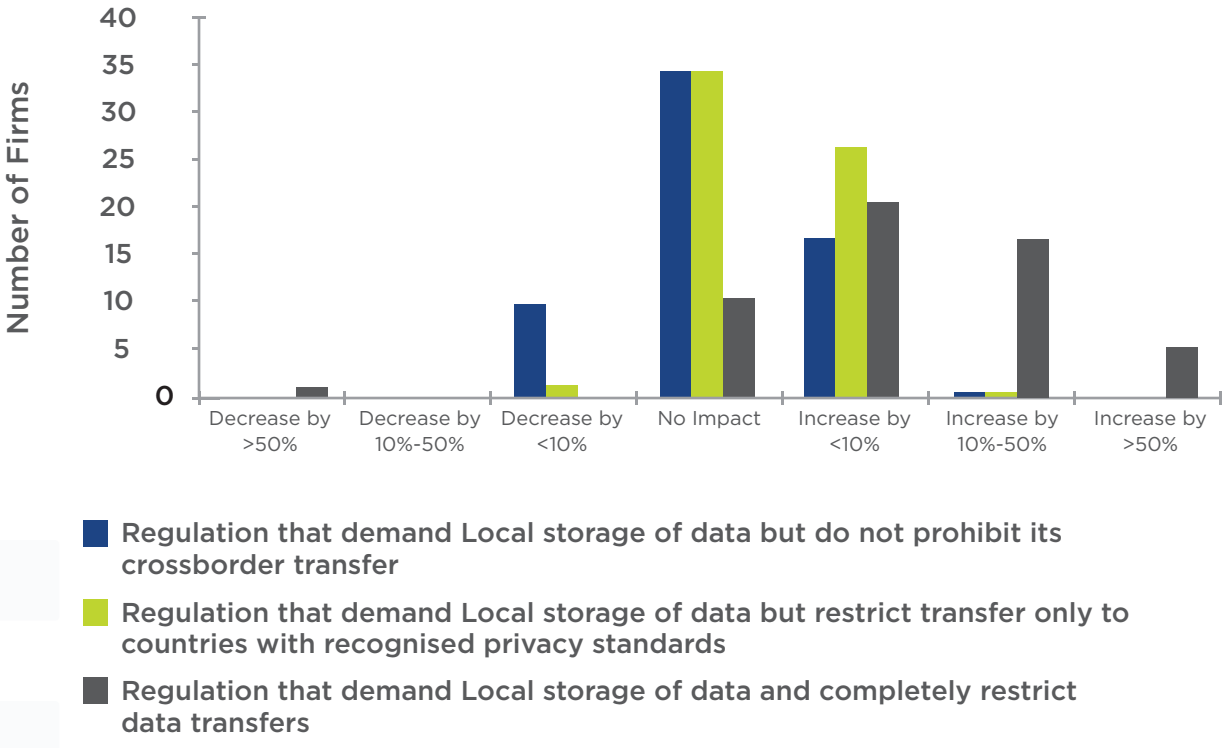


Figure 5.6: Impact on Data Management Costs if Proposed Data Localisation Measures are Implemented



In trying to understand the global scenario for data localisation policies and its impact on Indian businesses, we included a question in our survey seeking responses on whether firms were affected by data localisation measures in other countries. 32 percent firms reported being impacted by data localisation measures in other countries such as UK, USA, China, South Korea, EU, Canada, Australia and Singapore, among others. These were mostly firms of Indian origin with international operations. These companies belonging to the IT & telecom and banking, finance & insurance sectors stored their data overseas, in their own or outsourced servers as well as in their own servers in India. Some of these companies reported an increase in cost to downstream industries/ consumers as an outcome of data localisation policies in other countries. Castro and McQuinn (2015) illustrate the possibility of costs that can arise due to restrictions on cross border data flows in other countries. They take the example of retail and consumer goods firms like Tesco and Unilever. Due to restrictions on transfer of personal data, these firms might be forced to build additional data centres in each country of operation and the additional costs might then trickle down to customers.

This indicates that irrespective of where firms choose to locate their data, reciprocal or retaliatory data localisation measures in other countries are a potential threat to Indian businesses that either operate internationally or want to expand to other countries. Policies adopted by one country can quickly spiral a contagion of similarly drafted policies in other countries.

5.4 Business Perceptions on Data Localisation

The perception that data localisation would nurture domestic companies is strong among firms of Indian origin and operating only in India. There is an equally strong perception among firms of Indian origin that have operations outside India that data localisation would increase costs and increase the possibility of surveillance. Some firms reported that data localisation could potentially lower business efficiency and increase costs of operation for foreign firms, and the likelihood of the government to patronise domestic industry. These perceptions are inextricably linked to the context in which the respondent firm operates.

Figure 5.7: A: Benefits of Data Localisation to the Source Economy

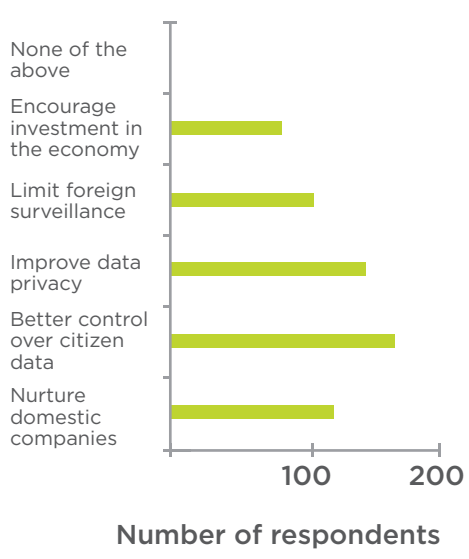
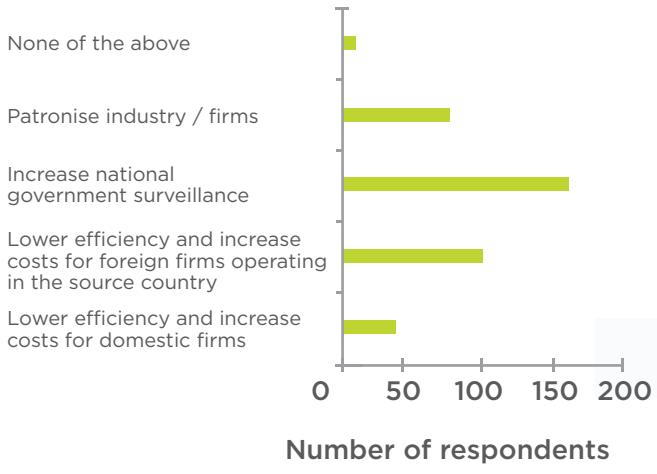


Figure 5.7: B: Costs of Data Localisation to the Source Economy



Finally, we asked our respondents their opinions on alternatives to restrictions on cross border data flows and data localisation. The use of bilateral agreements and softer versions of data localisation such as data mirroring were most popular, reinforcing the case study results. Due to the nature of the questionnaire, the nuances with respect to mirroring such as applicability by sector are not captured in the responses. Bilateral agreements with countries might reduce the risk of retaliatory measures and enable cooperation from partner countries minimising economic and legal conflict. Some other alternatives that respondents chose as a preference included industry based privacy frameworks and other horizontal reforms that improve the ease of doing business and naturally invite cloud companies and data centers to the country.

The survey reiterates the result that the impacts of data localisation on businesses both within and across sectors vary by the size of the company, the sector of operation, the choice of markets, business models, etc. Based on our analysis, firms in the IT, telecom and financial services sector are more affected than others. The report focuses on the economics of data localisation. If there are other government imperatives, but those which can be achieved without stringent restrictions on cross border data flows, such as those illustrated above, policy makers must consider them. To the extent that privacy or enforcement of law and order are not conceded.

6. Conclusions and Policy Recommendations

Global policy debates have been occupied with significant discussions on data localisation measures over the last few years. There are two divergent paths, one of extreme localisation as already practiced by China and Russia, and the other of complete free flows as advocated by the US. Countries place themselves in this continuum practicing both implicit and explicit forms of localisation. Localisation measures have either been imposed or proposed by a range of countries that differ by type of government, size or status of socio-economic well-being, etc. While several developing countries in Asia such as Vietnam and Indonesia have implemented stringent localisation measures, even developed countries such as Germany, France, Australia and Canada have implemented or are actively considering measures to regulate cross-border data flows.[109] These measures vary on the type of localisation, scope of localisation as well as the enforcement of the policy itself. However, the global discourse on data localisation has turned around after the G20 summit in Osaka in 2019. The framework of "Data Free Flow With Trust" presented by Japan, reaffirmed the interface between trade and the digital economy and the importance of promoting national and international policy discussions for harnessing the full potential of data and the digital economy to foster innovation.[110] Countries such as the US, EU, Australia, Singapore and Japan, pushed for the introduction of an international rule based system on cross-border data flows, and removal of prohibitions on free flow of data.[111] The Osaka declaration was signed by 50 countries[112], including countries like China and Russia, who have thus far imposed strict constraints on cross-border flow of data.[113] World leaders at the summit emphasized on the importance of digitally driven economies in spurring innovation and economic growth and the centrality of free flow of data to the digital ecosystem.[114] However, India, Indonesia and South Africa, along with other developing countries opposed the declaration and refused to sign on it, arguing that the plurilateral negotiations on digital trade strike at the root of a multilateral decision making process based on consensus, and undermined policy space for domestic measures.[115] However, Indonesia subsequently introduced a draft amendment to the data localisation requirement under its regulation of the Implementation of Electronics systems and Transactions.[116]

109. Refer to Appendix 1 for details on proposed and implemented regulations to cross-border data flows across the world
110. https://www.japantimes.co.jp/news/2019/06/28/national/abe-heralds-launch-osaka-track-framework-free-cross-border-data-flow-g20/#.XTlOZOgzaM8
111. https://www.medianama.com/2019/07/223-india-boycotts-osaka-track/
112. https://www.livemint.com/news/world/india-boycotts-osaka-track-at-g20-summit-1561897592466.html
113. See https://www.meti.go.jp/press/2019/06/20190628001/20190628001_01.pdf and https://g20.org/en/links/
114. https://indianexpress.com/article/india/g-20-osaka-summit-narendra-mod-india-declaration-on-free-flow-of-data-across-borders-shinzo-abe-5805846/
115. https://www.livemint.com/news/world/india-boycotts-osaka-track-at-g20-summit-1561897592466.html
116. https://www.linklaters.com/en/insights/publications/year-review-year-to-come/2018-2019/major-developments-in-indonesia-in-2018-and-2019

While the current rule in Indonesia requires its companies to store their data in a local data centre, under the amendment, the government is preparing to recognise different categories of data and apply different localisation requirements, based on those categories.[117]

Some consider the Snowden revelations in 2013 as a trigger for localisation across the globe. However, a closer examination of data localisation policies finds that such measures existed much before foreign surveillance and espionage concerns emerged. Most measures on localisation are driven by arguments that explain its role in enabling data privacy and smooth functioning of law enforcement agencies. Data localisation policies are also driven by economic interests; the critical use of data in business processes is driving countries to ring-fence data within their own borders. Several of the arguments in favour of data localisation find vociferous opposing views. The debate in India also finds two distinct camps - one that believes data localisation will improve security of Indian consumer data and contribute to the domestic digital ecosystem, and the other that claims that the costs of localisation will far surpass any gains from it. This study contributes to the domestic policy discussion by providing evidence on the economic impacts of data localisation in India.

Several studies have found the economic costs of data localisation to be significant. This is especially true given the passage of time and evolution of technology that has enabled globalization of business models. However, the impacts vary across countries, sectors of the economy and the scale of a business. We provide a macroeconomic assessment of data localisation in India by measuring the impact of cross-border data flows on India's international trade. India's foreign trade is an integral part of the country's growth process; exports create demand for domestic goods and generate benefits of scale and imports enable access to critical technology and other inputs. This study uses the gravity model of international trade to determine the impacts of cross-border data flows as measured by international internet bandwidth between India and its partner countries. The estimation finds that *if cross-border data flows were to decline by 1 percent, India's total trade could be negatively impacted by US$ 696.71 million*.

From interactions with stakeholders we have been able to draw a more nuanced assessment about impacts of data localisation measures on businesses across different sectors, sizes and types. The explicit costs include one-time costs for immediate investment in local infrastructure to comply with regulations. These are almost always accompanied by on-going or recurrent costs that include payments for upgradation of infrastructure or investments in new systems that maintain quality of service across different jurisdictions. Building and maintaining additional data storage facilities simply to comply with data localisation requirements, running those facilities often in less efficient network architectures, impose a significant cost burden on businesses. Implicit costs include the concern of reciprocity. In retaliation to India's localisation demands a similar or reciprocal measure in other countries could mean significant costs for Indian origin firms with global operations who store data in India.

Data localisation could entail loss of business not only for the company, but also the development of fewer innovative products and services in the country, and access to fewer products outside the country. On the other hand, the survey analysis also finds that not all traditional industries using data for enhancing the efficiency of its business processes, perceived their businesses to be impacted by localisation. Based on the survey responses, the impacts were found to be more concentrated for sectors such as IT, telecom and financial services which are completely data driven. While the sample sizes for both the case study analysis and the enterprise survey are not large enough to arrive at robust conclusions, the findings are indicative of the potential economic consequences of such a measure.

117. Ibid

Some policy recommendations are summarised below:

Encourage bilateral or plurilateral data transfer arrangements and soften data localisation measures through mirroring of select datasets: One of the most prominent motivations behind data localisation measures is access to data by local law enforcement agencies, or for any other lawful purpose as deemed necessary by the country. In this context, in addition to reforming the Mutual Legal Assistance Treaty System (MLAT System), it would be useful for India to explore bilateral or plurilateral data transfer arrangements, such as certification. Data transfer mechanisms like the US-EU Privacy Shield (bilateral) and APEC CBPR (multilateral) help ensure compliance with local laws, even when data is transferred outside the jurisdiction. Even for critical personal data, absolute data localisation requirements may not be necessary as long as the government is able to meet its objectives through such data transfer mechanisms. The Indian government should take note of globally recognised legal mechanisms for cross border data transfers, including mutual recognition of laws and practices, transfers based on certifications e.g. the APEC CBPR, codes of practice and contractual necessity. Other examples of such arrangements are the proposed e-evidence regulation in the EU and the CLOUD Act in the US. Imposing data localisation requirements on data fiduciaries would not, in itself, facilitate Indian law enforcement agencies' access to data from service providers outside the country. For example, the Electronics Communications Privacy Act (ECPA) currently bars US-based service providers from disclosing content of electronic communications to any law enforcement entity outside the US unless the requests are submitted via Mutual Legal Assistance Treaty or similar diplomatic and cooperative arrangements, between US and local law enforcement. Therefore, a potential conflict of law between US and Indian jurisdictions is likely to remain, which would not be resolved through any data localisation measures law enforcement access issues, if any, can be addressed through specific bilateral and multilateral instruments without resorting to data localisation measures. India could also consider mirroring of critical datasets that are critical in nature, as an option for ready access to data within the country's jurisdiction, instead of mandating complete localisation. The RBI Directive completely bans cross-border flow of data. Mirroring requirements allow for free flow of data while also providing local access of data to relevant authorities. The costs of mirroring are also lower than that of complete localisation. However, mirroring might be a prudent alternative only in the event where data transfer mechanisms fail to achieve the desired policy objectives.

Encourage international regulatory cooperation: Instead of mandating blanket localisation, countries could explore agreements or memorandums of understanding (MOU) between specific regulators across the globe to address specific issues of access to data, monitoring and safeguarding consumers' welfare and interests. There is a history of RBI to having entered into such MOUs with regulators in other countries, however the implementation or success of these MOUs are not well-known.

Minimise policy overlap: In order to address concerns of data privacy, the idea of an overarching framework that defines the general guidelines to safeguard privacy, is necessary. The draft Personal Data Protection Bill (2018) is a welcome change in this context. However, India is currently witnessing a host of proposed sectoral localisation measures that often overlap with existing policies, such as the Draft E-Commerce Policy, the draft e-pharmacy regulations etc. This results in potential over reach and over-regulation of the industry resulting in regulatory uncertainty.

Institutionalise consultative and transparent policy making processes: While most policy making in India has seen a process of consultation on occasions such as the RBI directive the consultation was completely missing. When policy making is consultative and transparent it is easier for stakeholders to understand the motivations, objectives and thinking that goes into formulation of the concerned policy. Moreover, regular communication enables them to comply better and share efficient alternatives.

Enable the overall IT ecosystem instead of forced data localisation: Forced localisation may not always achieve the stated economic or governance objectives. For example, the decision to host data servers is often driven by a complex combination of factors including the ease of scaling, availability of supporting infrastructure, etc. In India's current economic state, building local data centers may misallocate valuable resources resulting in loss of efficiency and suboptimal choices for global businesses. Forced data localisation, if at all, will help achieve the stated objectives at higher costs. On the other hand, policies that focus on the development of the overall ecosystem will organically invite localisation as businesses will find it more profitable and efficient to operate from India. This trend is already visible with several international cloud service providers expanding operations in India.

Evaluate risks of retaliatory measures and the potential fragmentation of the internet: With rising number of data localisation measures, it is possible that some countries that do not currently have data localisation measures may introduce retaliatory measures in response. While there are counter arguments, that suggest it would be in the interest of companies to comply in order to gain market access, reciprocal data localisation measures would not only risk healthy competition for consumers but also risk the fragmentation of the global internet. One of the features of the Internet that has made it a growth multiplier is its ability to allow services to scale globally at low costs. The fragmentation of the internet, would turn back the benefits of globalisation and isolate countries such as India, from the global value chains that make the data economies of today. The global nature of the digital economy has also enabled Indian startups to gain access to emerging technologies from across the world and reduce their IT costs. Retaliatory measures of localisation will limit these opportunities, thus hindering innovation and growth of startups.

Assess costs of delayed availability of latest services and updates in India and the negative impact on innovation: It may be noted that many global businesses would have to maintain dual set of infrastructures to comply with localisation measures in India. As a result, new services rolled out globally will need to be separately launched in India through Indian infrastructure. This could result in delays, and inadvertently affect consumer choice and competition in the market. Moreover, some companies are able to provide services in markets, in which establishing physical infrastructure might not be financially sustainable. Such companies would have to pull out of the Indian market or would be discouraged from potentially providing services in India because of the additional costs from data localisation.

Conduct Regulatory Impact Assessments (RIAs), security audits and vulnerability assessments before policy development and implementation: RIAs improve the quality of regulatory decision making by providing a complete picture of the potential pros and cons of a policy directive. RIAs are a common feature conducted by many regulators of various sectors in different countries. They could help policy makers by providing evidence on the impacts of an implemented policy, especially in an evolving digital industry with unprecedented regulatory needs. Further, data security audits and vulnerability assessments both for private businesses and public sector organisations, can help ensure the protection and privacy of data. This could be a viable alternative to sweeping data localisation measures.

Strengthen the overall cybersecurity framework as data localisation impedes globally coordinated security measures and fraud risk analysis: Data localisation measures affect the security measures, fraud and risk analysis involved in various financial services, for example. The utility of big data, and learning from global patterns of security threats, fraud etc. have led to improved cyber security practices, prevention of fraud and risk analyses. Fragmenting datasets would entail alterations in these processes. Moreover, in case such alterations are not possible, then the aforementioned practices would have to be foregone.

Bibliography

"Cross-Border Data Flows, Realising benefits and removing barriers". *GSMA* (2018)

"Demystifying the U.S. CLOUD Act: Assessing the law's compatibility with international norms and the GDPR". *Hogan Lovells (2019)*.

"The Digitization of the World From Edge to Core". *IDC, 2018*.

"The Localisation Gambit". *The Centre for Internet and Society (2019)*

"The Rise of Data Capital", MIT Technology Review Custom + Oracle

"Unleashing the benefits of free flow of data". *Telenor*, 2018

Aaronson, Susan Ariel, and Rob Maxim. "Data Protection and Digital Trade in the Wake of the NSA Revelations." *Intereconomics* 48 (2013).

Bailey, Rishab, and Smriti Parsheera. "Data localisation in India: Questioning the means and ends." *NIPFP Macro/Finance Group (forthcoming)* (2018).

Brynjolfsson, Erik, and Andrew McAfee. "The big data boom is the innovation story of our time." *The Atlantic* 21 (2011).

Brynjolfsson, Erik, and Andrew McAfee. *Race against the machine: How the digital revolution is accelerating innovation, driving productivity, and irreversibly transforming employment and the economy.* Brynjolfsson and McAfee, 2012.

Brynjolfsson, Erik, Lorin M. Hitt, and Heekyung Hellen Kim. "Strength in numbers: How does data-driven decision-making affect firm performance?" *Available at SSRN 1819486* (2011).

Carlsson, Bo. "The Digital Economy: what is new and what is not?." *Structural change and economic dynamics* 15, no. 3 (2004): 245-264.

Castro, Daniel, and Alan McQuinn. "Cross-border data flows enable growth in all industries. " *Information Technology and Innovation Foundation* 2 (2015): 1-21.

Chander, Anupam, and Uyên P. Lê. "Data nationalism." *Emory LJ* 64 (2014): 677.

Chander, Anupam. "Trade 2.0." *Yale J. Int'l L.* 34 (2009): 281.

Ciuriak, Dan, and Maria Ptashkina. "The Digital Transformation and the Transformation of International Trade." *RTA Exchange. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and the Inter-American Development Bank (IDB* (2018).

Cory, Nigel. *Cross-border data flows: Where are the barriers, and what do they cost?*. Information Technology and Innovation Foundation, 2017.

Gurumurthy, A., Vasudevan, A., &Chami, N. (2017). The grand myth of cross-border data flows in trade deals. IT for Change.

Hagedoorn, John. "Innovation and entrepreneurship: Schumpeter revisited." *Industrial and Corporate Change* 5, no. 3 (1996): 883-896.

Hart, Stuart L., and Mark B. Milstein. "Global sustainability and the creative destruction of industries." *MIT Sloan Management Review* 41, no. 1 (1999): 23.

Hill, Jonah. "The growth of data localisation post-snowden: Analysis and recommendations for us policymakers and business leaders." In *The Hague Institute for Global Justice, Conference on the Future of Cyber Governance*. 2014.

IAMAI-IMRB (2017). Digital Commerce Report

Kuner, Christopher. "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. *OECD Digital Economy Papers, 187*, (2011)

Manyika, J., S. Lund, J. Bughin, J. Woetzel, K. Stamenov, and D. Dhingra. "Digital Globalization: The New Era of Global Flows. New York: McKinsey Global Institute." (2016).

Martínez-Zarzoso, Inmaculada, and Felicitas Nowak-Lehmann. "Augmented gravity model: An empirical application to Mercosur-European Union trade flows." *Journal of applied economics* 6, no. 2 (2003): 291-316.

O'Connor, Brendan. "Quantifying the Cost of Forced Localization." *Leviathan Security Group, June* (2015).

Panday. Jyoti. Rising Demands for Data Localisation a Response to Weak Data Protection Mechanisms, Electronic Frontier Foundation, 2017

Pepper, Robert, John Garrity, and Connie LaSalle. "Cross-Border Data Flows, Digital Innovation, and Economic Growth." *The Global Information Technology Report 2016: Innovating in the Digital Economy* (2016): 39-40.

Sargsyan, T. (2016). Advancing Political and Economic Interests through Data Localisation in the Name of Privacy and Security. AoIR Selected Papers of Internet Research, 5.

Shapiro, Carl, and Hal R. Varian. *Information rules: a strategic guide to the network economy*. Harvard Business Press, 1998.

Terzi, Nuray. "The impact of e-commerce on international trade and employment." *Procedia-Social and Behavioral Sciences* 24 (2011): 745-753.

UNCTAD, 2016, Data protection regulations and international data flows:
United States International Trade Commission (USITC), Digital Trade in the U.S. and Global Economies, Part 1 (Washington, DC: USITC, July 2013)

Vemuri, Vijay K., and Shahid Siddiqi. "Impact of commercialization of the internet on international trade: A panel study using the extended gravity model." *The International Trade Journal* 23, no. 4 (2009): 458-484.

World Trade Report – The future of world trade: how digital technologies are transforming global commerce (2018)

Data Sources

TeleGeography
World Bank
IMF
Statista
WTO
UN Comtrade
CEPII Gravity Database

Appendix

Appendix

Appendix 1

Table A1.1: Regulations to Cross-Border Data Flows around the World

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Argentina	**Section 12 of the Data Protection Act of Argentina (Law 25,326)** prohibits the transfer of personal data to countries that do not have an adequate level of protection in place, but such countries have not been identified yet. The Regulatory Decree No. 1558/2001 provides that the prohibition is not applicable when the data subject has expressly consented to the transfer. Data can also be transferred to a foreign country by means of an international agreement between the data controller and the foreign processor, under which the latter undertakes to comply with the same standards of protection and other legal obligations as provided in the Argentine data protection regulations. A bill has been recently presented to Congress that would replace Law 25326 in order to align data protection standards with the GDPR.[118] Resolution 04/2019 aims 'to unify the criteria of the Agency of Access to Public Information for the correct interpretation and implementation of the current regulations on the protection of personal data, whose observance is mandatory.'	Personal Data[119]	Across all sectors	Active

118. https://www.moellerip.com/resolution-no-4-2019-argentina-begins-to-¨warm-up¨-for-the-law-of-personal-data/
119. https://gettingthedealthrough.com/area/52/jurisdiction/4/data-protection-privacy-argentina/

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Australia	**1. My Health Records Act 2012** requires local data centres to handle 'personally controlled electronic health records'. Therefore, no electronic health information can be held or processed outside Australia, unless they do not "include information in relation to a consumer" or they are "identifying information of an individual or entity". An Amendment passed in 2018 "removed the ability of the My Health Record System operator to disclose health information in My Health Records to law enforcement and government agencies without an order by a judicial officer or the healthcare recipient's consent; and require the system operator to permanently delete from the National Repositories Service any health information about a healthcare recipient who has cancelled their My Health Record."[120]	Health Data	Specific Sector	Active
	2. Under the **Federal Privacy Act**, before an organization discloses personal information to an overseas recipient, it must take reasonable steps to ensure that the overseas recipient will not breach the **Australian Privacy Principles (APPs)**. This requirement does not apply only if: - the overseas recipient is bound by a law similar to the APPs that the data subject can enforce; - the data subject consents to the disclosure of the personal data in the particular manner prescribed by APP; or - another exception applies. An organisation may be held liable for any breaches of the APPs by that overseas recipient. 13 APPs exist out of which APP 8 is concerned with "Cross-border Disclosure of Personal Information"[121]	Personal Data[122]	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.

120. https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r6169
121. https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information
122. https://www.oaic.gov.au/privacy-law/

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Belgium	**1. Article 463 of the Companies Code** requires that the company register of shareholders and register of bonds must be kept at the registered office of the company. Since 2005, it is possible to keep the registers in electronic format as long as they are accessible at the registered office of the company	Company Records	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.
	2. With respect to VAT, invoices received and copies of invoices issued by the taxpayer can be stored wherever the taxpayer wishes, yet they must be made available whenever the tax administration so requests. If the storage does not guarantee complete and online access, then mandatorily the invoices must be stored in Belgium.[123] Invoices must be stored either in electronic or paper format **(Article 60, § 3 of the VAT Code).**	Tax Data	Across all sectors	Active
	3. With respect to income tax, other than in cases of exception granted by the administration, the books and documents must be kept at the disposal of the tax administration in the office, agency, branch or other professional or private premises of the taxpayer where they have been kept, prepared or sent. **(Income Tax Code – Article 315)**	Tax Data	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.

123. https://www.lexology.com/library/detail.aspx?g=9337ef4a-139b-42be-b7e4-7e52fa9a8e79

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Belgium	**4.** There are no data localisation requirements under Belgian law. Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. Belgian data protection law supports all data-transfer mechanisms provided in the GDPR, including the use of standard contractual clauses, binding corporate rules, and the EU-U.S. Privacy Shield and accepts that data may be transferred on the basis of a derogation such as the individual's explicit consent. In principle, the individual concerned must be informed of the data transfer prior to the actual transfer, but **the Belgian DP Act** provides for exceptions in the area of law enforcement and intelligence services.	Personal Data and Non-Personal Data	Across all sectors	Active[124]
Brazil	**1.** In September 2013, Brazil began considering a policy that would have forced internet-based companies, such as Google and Facebook, to store data relating to Brazilians in local data centers. It withdrew this provision from the final copy of the bill. Furthermore, in 2016, Brazilian government agencies, including the Secretary of Information Technology of the Ministry of Planning, Development, and Management, have included forced data localisation as a requirement for public procurement contracts involving cloud-computing services.	Personal Data and Public Procurements	Across all sectors	Active

124. https://home.kpmg/be/en/home/insights/2018/11/belgian-data-protection-legislation-for-the-private-sector-broug.html

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Brazil	**2.** August 14, 2018, Brazil approved the **General Data Protection Law** which will come into effect after its 18th adaptation period, in August 2020. The LGPD creates a new legal framework for the use of personal data in Brazil, both online and offline, in the private and public sectors. Currently, Brazilian law does not provide any restrictions specific to international data transfers but once the LGPD starts to be applied it will only be possible (Article 33): - to countries or international organisations that provide adequate levels of data protection; - when the controller offers and proves compliance with the principles and rights of the data subject and the regime of data protection, upon specific contractual clauses, standard contractual clauses, global corporate rules or regularly issued stamps; - when the transfer is necessary for international legal co-operation between public intelligence, investigative and prosecutorial agencies; - when the transfer is necessary to protect the life or physical safety of the data subject or of a third party; - when the ANPD authorises the transfer; - when the transfer results in a commitment undertaken through international co-operation; - when the transfer is necessary for the execution of a public policy or legal attribution of public service; - when the data subject has given his or her specific consent for the transfer, with prior information about the international nature of the operation, with this being clearly distinct from other purposes; and	Personal Data[125]	Across all sectors	Will be applied from August 2020

125. https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Brazil	- when it is necessary to satisfy compliance with regulatory obligations by the controller, execution of a contract or preliminary procedures related to it and the regular exercise of rights in judicial, administrative or arbitration procedures.	Personal Data	Across all sectors	Will be applied from August 2020
Bulgaria	**1.** Under the **Gambling Act**, an applicant for a gaming license must ensure that all data related to operations in Bulgaria is stored on a server located in the territory of Bulgaria. Moreover, the applicant has to ensure that the communication equipment and the central computer system of the organiser are located within the EEA or in Switzerland		Specific Sector	Active
	2. Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. In view of the entry into force of Regulation (EU) 2016/679 (General Data Protection Regulation - 'GDPR'), on April 30, 2018 a draft law amending and supplementing the Personal Data Protection Act ('Draft Law') was introduced for public discussion. Public consultations ended on May 30, 2018 and the Draft Law was submitted to the Parliament where it is subject to further amendments.	Personal Data and Non-Personal Data	Across all sectors	Active

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Bulgaria	The Draft Law designates the Commission for Personal Data Protection as the sole supervisor responsible for protecting the fundamental rights and freedoms of individuals with regard to the processing and free movement of personal data within the European Union. The Draft Law further regulates the legal remedies in cases of violation of personal data law, the accreditation and certification in the field of personal data protection, the administrative liability and the administrative measures in cases of violations of the Draft Law. It entered into force on 2 March, 2019.[126]	Personal Data and Non-Personal Data	Across all sectors	Active
Canada	**1.** Nova Scotia requires that personal information held by a public body (primary and secondary school, universities, hospitals, government-owned utilities and public agencies) must be stored or accessed in Canada only. A public body may override the rules where storage or access outside of the respective province is essential. Moreover, the data can be transferred outside Canada "where the individual the information is about has identified the information and has consented, in the manner prescribed by the regulations, to it being stored in or accessed from, as the case may be, outside Canada".[127]	Personal Data held by Public Body	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.

126. https://home.kpmg/bg/en/home/insights/2019/02/bulgarian-data-protection-rules-take-further-shape.html
127. http://davidyounglaw.ca/cross-border-data-transfers/

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Canada	**2.** British Columbia requires that personal information held by a public body (primary and secondary school, universities, hospitals, government-owned utilities and public agencies) must be stored or accessed in Canada only. A public body may override the rules where storage or access outside of the respective province is essential. Moreover, the data can be transferred outside Canada "if the individual the information is about has identified the information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction".[128]	Personal Data held by Public Body	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.
	3. According to the Canadian Federal Law Personal Information Protection and Electronic Documents Act (PIPEDA) which is applicable to private sector organisations [129], consent is not necessary for the transfer of data to a third country as the Canadian law does not distinguish between domestic and international transfers of data. The company should, however, grant a comparable level of protection while the information is being processed by a third party. This is, preferably, achieved on a contractual basis with the third party.	Personal Data[130]	Across all sectors	No Data Localisation mandated, however comparable level of protection to be provided in foregin jursdiction

128. Ibid
129. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
130. https://digitalguardian.com/blog/what-pipeda-personal-information-protection-and-electronic-documents-act-understand-and-comply

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Canada	**4.** In 2006, Québec amended its Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information to require public bodies to ensure that information receives protection "equivalent" to that afforded under provincial law before "releasing personal information outside Québec or entrusting a person or a body outside Québec with the task of holding, using or releasing such information on its behalf"	Personal Data	Across all sectors	No Data Localisation mandated, however comparabale level of protection to be provided in foregin jursdiction
China	**1.** The "Notice to Urge Banking Financial Institutions to Protect Personal Financial Information" states that the processing of personal information collected by commercial banks must be stored, handled and analysed within the territory of China, and such personal information is not allowed to be transferred overseas. This is a pre-requisite in the Cyber Security Law.[131]	Financial Data	Specific Sector	Active. The implementing rules (18 May 2011) that clarify that PRC branches of foreign banks may transfer client information to their overseas headquarters, parent bank and subsidiaries for storage, processing and analysis if certain criteria are satisfied.

131. http://www.mondaq.com/china/x/561742/Security/Financial+Institutions+How+Far+Are+You+From+The+Cyber+Security+Law

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
China	**2.** According to Administrative Measures for Population Health Information, China (which is implemented on a trial basis), population health information needs to be stored and processed within China. In addition, storage is not allowed overseas.	Health Data	Specific Sector	Active[132]
	3. Under the Law of the People's Republic of China on Guarding State Secrets, the transfer of data containing state secrets abroad is prohibited.	Data containing State Secrets	Across all sectors	Active
	4. Under Interim Measures for the Administration of Online Taxi Booking Business Operations and Services, China instituted a licensing system for online taxi companies which requires them to host user data on Chinese servers.	User Data[133]	Specific sector	Active
	5. China has data residency laws that declare companies can store the data they collect only on servers in country	Multiple data types	Across all sectors	Active
	6. Under Map Management Regulations, online maps are required to set up their server inside the country and must acquire an official certificate.	Location and Map Data	Specific Sector	Active

132. https://www.lexology.com/library/detail.aspx?g=7084ad8e-0cf0-4cbd-b724-cf8e205e34e0
133. https://ecipe.org/dte/database/?country=CN&chapter=829&subchapter=

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
China	**7.** Under Administrative Regulations for Online Publishing Services (Online Publishing Regulations), strict guidelines for what can be published online and how the publisher should conduct business in China came into force in March 2016. According to the rules, any publisher of online content, including "texts, pictures, maps, games, animations, audios, and videos" will be required to store their "necessary technical equipment, related servers and storage devices" in China	Multiple data types[134]	Across all sectors	Active
	8. The Cybersecurity Law includes requirements for personal information of Chinese citizens and "important data" collected by "key information infrastructure operators" (KIIOs) to be kept within the borders of China. If there are business needs for the KIIOs to transfer this data outside of China, security assessments must be conducted. The definition of KIIOs remains to be finalised. On May 28, 2019, the Cyberspace Administration of China ("CAC") released draft Data Security Administrative Measures (the "Measures") for public comment. The Measures, which, when finalized, will be legally binding, supplement the Cybersecurity Law of China (the "Cybersecurity Law") that took force on June 1, 2017, with detailed and practical requirements for network operators who collect, store, transmit, process and use data within Chinese territory. The Measures likely will significantly impact network operators' compliance programs in China.[135]	Personal Data[136]	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.

134. Ibid
135. https://www.huntonprivacyblog.com/2019/06/10/china-issues-draft-of-data-security-administrative-measures/
136. Ibid

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
China	**9.** Article 5.4.5. of the Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems prohibit the transfer of personal data abroad without express consent of the data subject, government permission or explicit regulatory approval "absent express consent of the subject of the personal information, or explicit legal or regulatory permission, or absent the consent of the competent authorities". If these conditions are not fulfilled, "the administrator of personal information shall not transfer the personal information to any overseas receiver of personal information, including any individuals located overseas or any organizations and institutions registered overseas". Although the Guidelines are a voluntary technical document, they might serve as a regulatory basis for judicial authorities and lawmakers. The Personal Information Security Specification, which came into force in May 2018, also stresses that explicit consent is required when sensitive data is being collected. The Specification is not a legally binding text, but the Chinese government agencies are likely to refer to it as a standard to determine whether companies are following China's data protection rules.[137]	Personal Data	Across all sectors	Active. However, the guidelines are voluntary.

137. https://www.insideprivacy.com/data-security/chinas-ministry-of-public-security-issues-new-personal-information-protection-guideline/

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Colombia	Pursuant to Law 1266 of 2008, personal data may not be transferred outside of Colombia to countries which do not comply with the adequate standards of data protection. This restriction does not apply in the following cases: - when there is an express authorisation by the data subject; - when the information relates to medical data as required by issues of health and public hygiene; - for banking operations; and - for operations carried out in the context of international conventions which Colombia has ratified. "Statutory Law 1581 of 2012 (Law 1581) regulates personal data processing, as well as databases. Law 1581 is applicable to all data collection and processing in Colombia, except data regulated under Law 1266 and certain other types of data or regulated industries. Decree 1377 of 2013 (Decree 1377), is a piece of secondary regulation related to Law 1581 which outlines requirements for personal and domestic databases regarding authorization of personal data usage and recollection, **limitations to data processing, cross-border transfer of data bases and privacy warnings, among others**. This Decree also requires that controllers and processors to adopt a privacy policy and privacy notice."[138]	Personal Data[139]	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.

138. https://www.dlapiperdataprotection.com/index.html?t=law&c=CO
139. https://www.dlapiperdataprotection.com/index.html?t=law&c=CO

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Cyprus	Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. The Protection of Physical Persons Against the Processing of Personal Data and Free Movement of such Data Law 125(I)/2018, that implements certain provisions of the GDPR into local law, entered into force on July 31, 2018 (the "**Law**").	Personal Data[140] and Non-Personal Data	Across all sectors	Active
Denmark	**1.** The basis of the Bookkeeping Act (section 12) is that accounting records in electronic form can be stored in Denmark or abroad if a certain set of conditions are met.[141] Hence, if financial records are stored on a server physically placed outside Denmark a complete copy must be kept in Denmark. (Consolidated Act No. 648 of 15 June 2006 (Bookkeeping Act)	Company Records (Financial)	Across all sectors	Active
	2. The basis for the Audit Act (section 45) is that financial records for governmental institutions must be stored in Denmark. This applies to both physical appendixes and digital data. This regulation means that financial records may be stored on a server abroad provided that an exact copy of the records is made on a monthly basis at a minimum. Such copy must be placed on a server in Denmark or in paper. (Consolidated Act No. 1035 of 21 August 2007 (Audit Act)	Government Data (Financial)	Specific sectors	Active

140. https://iclg.com/practice-areas/data-protection-laws-and-regulations/cyprus
141. https://www.bdo.dk/getmedia/75e9b9f2-319e-4b97-b5c6-34b3c54f6b5d/the-danish-bookkeeping-act-and-the-enterprise-2015.pdf.aspx

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Denmark	**3.** Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. To implement the GDPR, the Danish Parliament enacted the Danish Act on Data Protection (the 'Danish Data Protection Act') on May 17, 2018, enforceable on May 25, 2018 and replacing the previous Danish Act on Processing of Personal Data (Act no. 429 of 31/05/2000). Hence, data protection and processing in Denmark is now regulated by the GDPR as supplemented by the Danish Data Protection Act. The Danish Data Protection Act does not apply to Greenland and the Faroe Islands.	Personal Data and Non-Personal Data[142]	Across all sectors	Active
European Union	**1.** The European Union has updated its data protection regime by replacing the Directive 95/46/ EC with the General Data Protection Regulation (GDPR). The Regulation was approved in April 2016 and it has been in force with immediate effect on all 28 EU Member States from 25 May 2018.	Personal Data[143]	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.

142. https://www.datatilsynet.dk/english/legislation/
143. https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
European Union	**2.** Formally adopted on 14 November 2018 by the European Parliament and the Council's, the Regulation (EU) 2018/1807 is a framework for the free flow of non-personal data in the European Union. It is the follow-up to GDPR and is another major pillar in the EU's drive to create a Digital Single Market. Non-personal data' is defined as any data that doesn't constitute personal data under Article 4 of GDPR. The prominent change being introduced by Regulation (EU) 2018/1807 is that member states will be prohibited from enforcing data localisation in relation to the processing or storing of non-personal data. The aim of this is to promote the free movement of non-personal data across the EU without any interference from member states. The only exemption from this prohibition comes in the form of restrictions on movement when necessary for public security. In order to avail of this exemption, the relevant member state must communicate any remaining or proposed data localisation policies to the European Commission along with their justifications for the restriction.	Non-Personal Data[144]	Across all sectors	Active since 28th May, 2019[145]
Finland	The Accounting Act 1366/1997 requires that a copy of the accounting records in kept within Finland. Alternatively, the records can be stored in another EU country if a real-time connection to the data is guaranteed.	Company Records	Across all sectors	Active

144. https://www.wiggin.co.uk/insight/eu-regulation-2018-1807-eu-on-the-framework-for-the-free-flow-of-non-personal-data-in-the-eu-published-in-official-journal/
145. http://www.mondaq.com/uk/x/818470/data+protection/European+Commission+Issues+Guidance+On+The+Free+Flow+Of+NonPersonal+Data+In+The+EU

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Finland	Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. Finland has passed a supplementary implementation act of the GDPR, the Data Protection Act of Finland (Tietosuojalaki), which repeals the Personal Data Act (523/1999), as well as the Law on the Data Protection Board and the Data Protection Commissioner (389/1994). The Data Protection Act of Finland entered into force on 1 January, 2019.[146]	Personal Data and Non-Personal Data	Across all sectors	Active
France	**1.** A ministerial circular dated 5 April 2016 on public procurement states that it is illegal to use a non- "sovereign" cloud for data produced by public (national and local) administration: all data from public administrations have to be considered as archives and therefore stored and processed in France. (Ministerial Circular from 5 April 2016 - Note d'information du 5 avril 2016 relative à l'informatiqueennuage (Cloud computing))	Multiple data types	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.

146. https://www.dataguidance.com/finland-new-data-protection-act-enters-into-force-after-being-significantly-delayed/

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
France	**2.** Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. France adapted its domestic legislation to GDPR with the enactment of (i) Law No.2018-493 of June 20, 2018 on the protection of personal data, which mainly updates Law No. 78-17 of January 6, 1978 on information technology, data files and civil liberties, the principal law regulating data protection in France (the "**Law**") and (ii) Decree No. 2018-687 of 1 August 2018 implementing the Law, which updates the Decree No. 2005-1309 of 20 October 2005 (the "**Decree**"). In addition, the Order No. 2018 of December 12, 2018, adopted pursuant to Article 32 of Law No. 2018-493, updates the Law and other French laws relating to personal data protection in order to "*simplify the implementation and make the necessary formal corrections to ensure consistency with EU data protection law*" (the "**Order**"). The Order will enter into force on June 1, 2019. The Decree will be amended before June 1, 2019 by another decree, in order to take into account the revisions introduced by the Order. In addition, French rules adopted on the basis of the leeway left to Member States by the GDPR will apply only to the extent the data subject resides in France, including when the data controller is not established in France, with an exception for processing carried out for journalistic purposes or the purpose of academic, artistic or literary expression. For such processing activities, the national rules of the Member State where the data controller is established apply, to the extent such controller is established in the European Union.	Personal[147] and Non-Personal Data	Across all sectors	Active

147. https://www.dlapiperdataprotection.com/index.html?t=law&c=FR&c2=

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Germany	**1.** The Act on Value Added Tax states that invoices must be stored within the country, including when stored electronically. Alternatively, in case of electric storage, they may be stored within the territory of the EU if full online access and the possibility of download are guaranteed. In this case, the entity is obliged to notify the competent tax authority in writing of the location of the electronically stored invoices, and the tax authority may access and download the data. (Act on Value Added Tax - Section 14b) (Umsatzsteuergesetz, UStG)	Tax Data	Across all sectors	Active
	2. Under the Tax Code Section 146(2) 1, all persons and companies liable to pay taxes that are obliged to keep books and records must keep those records in Germany. There are some exceptions for multinational companies.	Tax Data	Across all sectors	Active
	3. According to the German Commercial Code Section 257 No. 1 and 4 (Handelsgesetzbuch § 257), accounting documents and business letters must be stored in Germany.	Company Records	Across all sectors	Active

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Germany	**4.** Under the Directive on Data Retention, operators were required to retain certain categories of traffic and location data (excluding the content of those communications) for a period of between six months and two years and to make them available, on request, to law enforcement authorities for the purposes of investigating, detecting and prosecuting serious crime and terrorism. On 8 April 2014, the Court of Justice of the European Union declared the Directive invalid. However, not all national laws which implemented the Directive have been overturned. In 2010, the German Constitutional court found the implementation of the Directive on Data retention to be unconstitutional. Yet, in October 2015, a new data retention law was passed, which will enter into force in 2017. The law provides that telecommunication providers must retain data such as phone numbers, the time and place of communication (except for emails), and the IP addresses for either four or 10 weeks. The data is to be stored in servers located within Germany (§113b). (German Telecommunications Act, as amended in December 2015)	Telecommunicat-ions Data	Specific sectors	Active

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Germany	**5.** Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. Germany has adjusted the German legal framework to the GDPR by passing the new German Federal Data Protection Act (Bundesdatenschutzgesetz – 'BDSG'). The BDSG was officially published on July 5, 2017 and came into force together with the GDPR on May 25, 2018. The purpose of the BDSG is especially to make use of the numerous opening clauses under the GDPR which enable Member States to specify or even restrict the data processing requirements under the GDPR.	Personal[148] and Non-Personal Data	Across all sectors	Active
Greece	**1.** In Greece, the Law No. 3971/2011 goes further in the implementation of the Data Retention Directive (later annulled by the European Court of Justice) by requiring that retained data on 'traffic and localisation' stay 'within the premises of the Hellenic territory'. The Law is still in force.	Multiple data types	Across all sectors	Active

148. https://www.dlapiperdataprotection.com/index.html?t=law&c=DE&c2=

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Greece	**2.** Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. The main set of data protection rules consists of L. 2474/1997, which harmonized the Greek legislation with Directive 95/46/EC. This law sets out the obligations of those who process personal data and the respective rights of those to whom the data processing relates. The same Law also provides for the establishment of the Hellenic Data Protection Authority (HDPA) and its powers and competencies A bill of law (the 'Bill') was published on February 20, 2018 which was submitted to public consultation. It should be noted that such Bill provides for both the legal measures implementing the Regulation 2016/679 (GDPR) in Greece, as well as the integration into the Greek legal order Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. However the Bill has not been enacted yet.[149]	Personal[150] and Non-Personal Data	Personal and Non-Personal Data	

149. http://www.greeklawdigest.gr/topics/data-protection/item/111-personal-data-protection
150. http://www.greeklawdigest.gr/topics/data-protection/item/111-personal-data-protection

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
India	**1.** The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules provide that cross-border data flows of sensitive personal data or information can be made: - provided that such transfer is necessary for the performance of a lawful contract between the body corporate (or any person acting on its behalf) and the provider of information, or - provided that such transfer has been consented to by the provider of information.	Personal Data	Across all sectors	Active
	2. In 2012, India enacted a "National Data Sharing and Accessibility Policy", which effectively means that government data (data that is owned by government agencies and/or collected using public funds) must be stored in local data centres. Moreover, Section 4 of the Public Records Act of 1993 already prohibited public records from being transferred out of Indian territory, except for 'public purposes'. It provides: "No person shall take or cause to be taken out of India any public records without prior approval of the Central Government: provided that no such prior approval shall be required if any public records are taken or sent out of India for any official purpose".	Multiple data types	Across all sectors	Active

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
India	**3.** On August 24, 2017, a Constitutional Bench of nine judges of the Supreme Court of India in Justice K.S.Puttaswamy (Retd.) v. Union of India [Writ Petition No. 494/ 2012] upheld that privacy is a fundamental right, which is entrenched in Article 21 [Right to Life & Liberty] of the Constitution. This led to the formulation of a comprehensive Personal Data Protection Bill 2018. The PDP Bill proposes to permit cross-border transfer of personal data and SPD subject to certain conditions, including data localisation and the transfer being subject to the DPA's approval.Furthermore, the PDP Bill recommends the localisation of at least one serving copy of personal data in India and that SPD will be stored only in servers located in India. The PDP Bill includes a new rule issued by the Reserve Bank of India (RBI) for payment systems providers operating in the country. Under the rule, all user data collected within the borders of the country needed to be localized within six months. The RBI said it was motivated by the need to have "unfettered supervisory accesses" to such data, given the fast-growing and increasingly technology dependent payments ecosystem in India.	Personal Data	Across all sectors	

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Indonesia	**1.** Regulation 82 of 2012 regarding the Provision of Electronic System and Transaction states that the storing of personal data and performing a transaction with the data of Indonesian nationals outside the Indonesian jurisdiction is restricted. This requirement appears to refer to personal data and transaction data of Indonesian nationals which is used within Indonesia and/or related to Indonesian nationals in particular. The Regulation targets "electronic systems operators for public services", whose definition remains unclear.	Personal Data	Across all sectors	Active
	2. In Indonesia, data protection is covered by Law No. 11 of 2008 regarding Electronic Information and Transaction (EIT Law) and Government Regulation No. 82 of 2012 regarding the Provision of Electronic System and Transaction (Regulation 82), which went into force on 15 October 2012. Regulation 82 requires "electronic systems operators for public service" to set up a data centre and disaster recovery centre in Indonesian territory for the purpose of law enforcement and data protection. In January 2014, the Technology and Information Ministry circulated a Draft Regulation with Technical Guidelines for Data Centers. The unclear and possibly all-encompassing definition of public services gave rise to concerns when a spokesperson was quoted saying: "[the draft] covers any institution that provides information technology-based services." Data carriers covered by these provision, therefore, would include a wide range of actors such as cloud providers, foreign banks and mobile phone providers. A government plan to amend this law is in process.[151]	Multiple Data Types	Across all sectors	Active

151. https://www.thejakartapost.com/news/2019/02/08/stakeholders-at-crossroads-amid-uncertainty-in-data-management. html ; Also see: https://www.lexology.com/library/detail.aspx?g=a116020b-cee3-433f-b62b-a5e988477d8e

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Indonesia	**3.** In the Annex of Circular Letter of Bank Indonesia No. 16/11/DKSP Year 2014 regarding E-money Operations, there is a requirement for all operators of e-money to localise data centres and data recovery centres within the territory of Indonesia.	Financial Data	Specific sectors	Active
	4. A new draft Bill on the Personal Data Protection Act (PDP) being discussed and as of this date it has not been issued. Although the exact date remains uncertain and the Bill is still to be considered by the House of Representatives, if passed, this will become Indonesia's first comprehensive law to specifically deal with the issue of data privacy.[152]			Proposed
Iran	On July 2018, Iran have released the first draft of the Personal Data Protection and Safeguarding Bill. The Draft Bill outlines data subject rights, the obligations of controllers and processors, offences and punishment, and provides for the establishment of a supervisory authority, which will be tasked with receiving and processing stakeholder's complaints regarding personal data.[153] The ICT Minister also expressed his contentment about the GDPR (General Data Protection Regulation) and, in the near future, he will conduct talks with the EU about mutual legal and technical assistance.	Personal Data		Proposed

152. https://www.opengovasia.com/indonesia-drafts-personal-data-protection-act/
153. https://www.article19.org/resources/iran-data-protection-draft-act/

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Iran	Iran it has been slowly moving toward developing its own national intranet—the Halal Internet—to separate itself (as best it can) from the rest of the internet, including moves toward greater data localisation. Iran's government operates an extensive online censorship regime. During political protests in 2009, Iran blocked Facebook, Twitter, and YouTube. In 2015, Iran launched its own search engines, which only show approved websites. In August 2016, Iran set up its first government-paid cloud data center. In May 2016, Iran ordered foreign messaging apps, such as WhatsApp and Telegram, to store data from Iranian users locally.[154]	Messaging and Communications Data	Specific sectors	Active
Kazakhstan	Since 2005, Kazakhstan has required that all domestically registered domain names (i.e., those on the ".kz" top-level domain) operate on physical servers within the country). The main legal act regulating personal data in Kazakhstan is the law of the Republic of Kazakhstan No. 94-V dated May 21, 2013 'On Personal Data and Its Protection' (the 'Law'). There are also a number of other laws providing for personal data protection requirements, including:[155] • The Law on Informatisation • The Law on Communication • The Labour Code of Kazakhstan	Personal Data	Across all sectors	Active

154. http://www.europarl.europa.eu/doceo/document/E-8-2016-004797_EN.html
155. https://www.dlapiperdataprotection.com/index.html?t=law&c=KZ

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Kazakhstan	Furthermore, in 2015, Kazakhstan enacted an amendment to its personal data-protection law that requires owners and operators collecting and using personal data to keep such data in-country. The requirement for localisation of personal data applies to companies established in Kazakhstan and individual proprietors in Kazakhstan, including branches and representative offices of foreign companies. It is not clear whether the localisation requirement should apply to foreign companies without any legal presence in Kazakhstan but whose websites are accessible in Kazakhstan.	Personal Data	Across all sectors	Active
Kenya	In June 2016, Kenya released its draft National Information and Communications Technology Policy, which aims to update the government's efforts to revise ICT-related economic policy. In the section on data centers, under the title of policy objectives, the report states that policy should "facilitate the development and enactment of legislation to support growth in IT service consumption—as an engine to spur data center growth." Currently, there are two draft data protection bills under consideration, which are separately undergoing legislative process and stakeholder consultation. As of now it is unclear whether one of these bills will ultimately be passed. There are various legal sources that address data protection including the Health Act 2017 and the Computer Misuse and Cybercrimes Act 2018.		Across all sectors	

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Luxembourg	**1.** According to the Circular CSFF 12/552 (as amended by Circulars CSSF 13/563 and CSSF 14/597), financial institutions in Luxembourg are required to process their data within the country. Processing abroad is exceptionally permitted for an entity of the group to which the institution belongs or with explicit consent.	Messaging and Communications Data	Specific sectors	Active
	2. Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. Two Luxembourg Data Protection Laws of August 1, 2018 have been enacted to implement the GDPR. The first law (the Luxembourg Data Protection Law) defines the organisation of the Luxembourg data protection authority (the CNPD) and provides for specific requirements or exceptions in implementation of the GDPR. it should be noted that the Luxembourg Data Protection Law specifically prohibits the processing of genetic personal data in the field of employment law and insurance. The second law (the Luxembourg Law on Criminal Data Processing) specifically relates to the protection of individuals with regard to the processing of personal data in criminal matters and national security.[156]	Financial Data	Across all sectors	Active

156. https://www.lexology.com/library/detail.aspx?g=3013cc14-25e2-4435-9e6d-24838132b58d

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Malaysia	The Personal Data Protection Act 2010 (PDPA) does not permit a data user to transfer any personal data out of Malaysia. However, the Act offers a set of exceptions, permitting the transfer of data abroad under certain conditions. The transfer is allowed if: - the data subject has given his consent to the transfer; - the transfer is necessary for the performance of a contract between the data subject and the data user; - the transfer is necessary for the conclusion or performance of a contract between the data user and a third party that is either entered into at the request of the data subject or in his interest; - the transfer is in the exercise of or to defend a legal right; - the transfer mitigates adverse actions against the data subjects; - reasonable precautions and all due diligence to ensure compliance to conditions of the Act were taken; or - the transfer was necessary for the protection the data subject's vital interests or for the public interest as determined by the Minister. PDPA was passed by the Malaysian Parliament on June 2, 2010 and came into force on November 15, 2013.[157] However, Malaysia is planning to amend its data protection laws to introduce a data breach notification regime and a wide expansion of the rights of data subjects. The Communications and Multimedia Minister has stressed the need for a refresh of the legislation, in a process that should take the EU's General Data Protection Regulation (GDPR) into consideration.[158]	Personal Data	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.

157. https://www.dlapiperdataprotection.com/index.html?t=law&c=MY
158. https://www.lexology.com/library/detail.aspx?g=3d6cc7f0-ea34-426d-9b3e-d696159a3abb

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
The Netherlands	**1.** Under the Public Records Act, localisation requirements apply to public records that have to be stored in archives in specific locations in the Netherlands. This applies both to paper and electronic records.	Public Records	Across all sectors	Active
	2. Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. The Dutch GDPR Implementation Act (*Uitvoeringswet AVG*, the **Implementation Act**) constitutes the local implementation of the GDPR in the Netherlands. The Implementation Act follows a policy-neutral approach, meaning that the requirements of the previous Dutch Data Protection Act (*Wet bescherming persoonsgegevens*) are maintained insofar as possible under the GDPR. The Implementation Act provides for, among other things, national rules where this is necessary for the implementation of GDPR provisions on the position of the regulatory authority or the fulfilment of discretionary powers provided by the GDPR.	Personal and Non-Personal Data	Across all sectors	Active

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Nigeria	**1.** At the beginning of 2014, the National Information Technology Development Agency (NITDA) released Guidelines on Nigerian Content Development in Information and Communications Technology. One of the requirements imposes that "Data and Information Management Firms" host government data locally within the country and shall not for any reason host any government data outside the country without an express approval from NITDA and the Secretary of Federal Government. Another requirement imposes that all ICT companies host their subscriber and consumer data locally.	Multiple data types[159]	Across all sectors	Active
	2. The Guidelines on Point-of-Sale Card Acceptance Services require IT infrastructure for payment processing to be located domestically. All Point-of Sale and ATM domestic transactions need to be processed through local switches and it is forbidden to route transactions outside the country for processing.	Financial Data	Specific Sector	Active

159. https://nitda.gov.ng/wp-content/uploads/2018/08/Guidelines-for-Nigerian-Content-Development.pdf

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Nigeria	**3.** NITDA issued the Nigeria Data Protection Regulation 2019 ("The Regulation") on 25th January, 2019. It was enforced on the same day. The Regulation regulates the activities of Data Controllers and Data Administrators in their use of the personal data of all natural persons who are Nigerian citizens (**Nigerian Citizens**) or who live in Nigeria (**Nigerian Residents**) and several concepts have drawn precedents from the GDPR. Personal data may only be processed if at least one of five legal bases are met: (1) the data subject provides consent, or if the processing is necessary; (2) for the performance of a contract; (3) to meet a legal obligation; (4) to protect the vital interests of the data subject; or (5) for the performance of a task carried out in the public interest. Transfer of personal data outside Nigeria is allowed only if certain specified criteria is met.[160]	Personal Data		Active
New Zealand	**1.** New Zealand's Inland Revenue Service issued a "Revenue Alert" stating that companies were required to store business records in data centres physically located in New Zealand in order to comply with the Inland Revenue Acts.	Company Records	Across all sectors	Active

160. http://www.mondaq.com/Nigeria/x/791990/Data+Protection+Privacy/Nigerias+2019+Data+Protection+Regulation+A+Fair+Scale+For+Privacy+And+Commercial+Rights ; https://www.huntonprivacyblog.com/2019/04/05/nigeria-issues-new-data-protection-regulation/

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
New Zealand	**2.** Consent is not required for the transfer of data to third countries, subject to compliance with the Information Privacy Principles. However, both the Privacy Act 1993 and the Health Information Privacy Code continue to apply to personal information and health information even when it is transferred out of New Zealand. The Privacy Commissioner is given the power to prohibit a transfer of personal information from New Zealand to another state, territory, province or other part of a country by issuing a transfer prohibition notice. A Privacy Amendment Bill was introduced to New Zealand's parliament in 2018 which repeals and replaces the Privacy Act 1993, as recommended by the Law Commission's 2011 review of the Act. The bill is undergoing a second reading in the legislature and if enacted, it will include stronger powers for the Privacy Commissioner, mandatory reporting of privacy breaches, new offenses and increased fines.[161, 162, 163]	Personal Data	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.
Poland	**1.** According to the Polish Gambling Act, any entity organizing gambling activities is obliged to archive all d a t a exchanged between such entity and the users in an archive device located in Poland in real time. Another restriction is the requirement that the equipment (servers) for processing and storing information and data regarding the bets and their participants must be installed and kept on the territory of a member state of the EU or EFTA.		Specific Sector	Active

161. https://www.parliament.nz/en/pb/bills-and-laws/bills-proposed-laws/document/BILL_77618/privacy-bill
162. https://www.dlapiperdataprotection.com/index.html?t=law&c=NZ
163. http://www.mondaq.com/NewZealand/x/764004/data+protection/Introduction+to+the+Privacy+Bill+2018+mandatory+reporting+of+privacy+breaches

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Poland	**2.** Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. Two new pieces of legislation are aimed at implementing the GDPR into the Polish legal order, as well as regulating the matters in which the GDPR leaves a certain regulatory freedom for EU Member States. The first one was the draft of the PDPA which came into force on May 25, 2018 (Personal Data Protection Act of 10 May 2018 (Journal of Laws of 2018, item 1000, hereinafter referred to as the new PDPA), while the second is the draft act on the provisions implementing the new PDPA (it contains a number of amendments of sectorial regulations (hereinafter referred to as the draft of the second act). The entry into force of the draft of the second act has been delayed and, according to the latest information, the legislative procedure may not be completed before late 2019. The new PDPA establishes a new supervisory body – the President of the Office for Personal Data Protection (hereinafter referred to as the President of the Office), which has a much wider range of powers than the previous DPA (Inspector General for the Protection of Personal Data – hereinafter referred to as the Inspector General). The Personal Data Protection act was further amended on 4th May 2019. As per the amendments, the Polish DPA will obtain additional powers: the DPA will be able to demand from the controller any information necessary to determine the basis for calculating the penalty. The scope of required information will be determined by the DPA, who may request, for example, financial data of the company. Also, the controller will be allowed to appoint a deputy data protection officer (DPO) for periods of absence of the designated DPO.[164]	Personal and Non-Personal Data	Across all sectors	Active

164. https://www.lexology.com/library/detail.aspx?g=72ef23b7-21a3-40a2-af47-358bbec80177

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Romania	**1.** According to law no. 124 from May 2015, regarding the approval of the Government Emergency Ordinance no. 92/2014 regulating fiscal measures and modification, the game server (gambling) must store all data related to the provision of remote gambling services, including records and identification of the players, the stakes placed and the winnings paid out. Information must be stored using data storage equipment (mirror server) situated on Romanian territory.		Specific Sector	Active
	2. According to the law on the protection of individuals with regards to the processing of personal data and the free movement of such data (Data Protection Law), any transfer of personal data to any state requires prior notification to the National Supervisory Authority for Personal Data Processing (NSAPDP). Moreover, any transfer of personal data to a recipient state not offering an adequate level of protection needs prior approval.	Personal Data	Across all sectors	Active
	3. Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. Law no. 190/208 published and applicable on July 31, 2018 constitutes the application of the GDPR into legal order. Law no. 190/2018 regulates, among others, the following activities, in addition to providing a framework related to the sanctions applicable to public authorities and public bodies:	Personal and Non-Personal Data	Across all sectors	Active

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Romania	Processing of genetic data, biometric data or health data ; Processing of a national identification number ; Processing of personal data in the context of employment relationships ; Processing of personal data and of special categories of personal data within the performance of a task carried out in the public interest.			
Russia	**1.** Federal Law no. 152-FZ "On Personal Data" (OPD-Law) as amended in July 2014 by Federal Law No. 242-FZ: Russian data protection has been covered since 27 July 2006 by Federal Law no. 152-FZ, also known as the OPD-law ("On Personal Data"). In July 2014, the law was amended by the Federal Law No. 242- FZ to include a clear data localisation requirement. Article 18 §5 requires data operators to ensure that the recording, systematisation, accumulation, storage, update/amendment and retrieval of personal data of the citizens of the Russian Federation is made using databases located in the Russian Federation. This amendment entered into force on 1 September 2015. It is not clear how restrictive the data localisation requirement is, but it appears that the OPD-Law does not prohibit accessing the servers from abroad and does not impose any special restriction on cross border data transfers or duplication of personal data. Online websites that violate the prohibition could be placed on the Roscomnadzor's blacklist of websites.	Personal Data[165]	Across all sectors	Active

165. https://emasglobe.com/sites/default/files/legal/the-privacy-policy.pdf

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Russia	**2. Federal Law No. 161-FZ** "On the National Payment System" dated June 2011 (the NPS Law) as amended in October 2014 by the Federal Law No. 319-FZ "On Amendments to the Federal Law on the National Payment System and Certain Legislative Acts of the Russian Federation": The amendments to the National Payment System Law require international payment cards to be processed locally. The law requires international payment systems to transfer their processing capabilities with respect to Russian domestic operations to the local state-owned operator (National Payment Card System) by 31 March 2015. The amendments are reported to be a response to the international political sanctions which prohibited certain international payment systems (e.g., Visa and MasterCard) from servicing payments on cards issued by sanctioned Russian banks.	Financial Data	Specific Sector	Active
	3. The "Blogger's law" requires "organizers of information distribution in the internet" (it is not clear which operators fall under this definition) to store on Russian territory information on facts of receiving, transfer, delivery and/or processing of voice information, texts, images, sounds and other electronic messages and information about users during six months from the end of these actions. Blogs with more than 3,000 readers are required to register as "organizers of information distribution" and are therefore subject to this requirement. Platforms that do not comply with these requirements upon a second notice face a fine of 500,000 rubles (approx. 900 USD) and can be blocked in Russia by Roscomnadzor. Russian services such as VKontakte, Yandex and Mail. Ru already registered their activities.	Multiple data types[166]	Across all sectors	Active

166. https://www.bbc.com/news/technology-28583669

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Russia	**4.** Government Decree No. 758 of 31 July 2014 and No. 801 from 12 August 2014: The Russian Government has given instructions to require public Wi-Fi user identification. The government decrees require that: - ISPs should identify internet users, by means of identity documents (such as a passport); - ISPs should identify terminal equipment by determining the unique hardware identifier of the data network; - all legal entities in Russia are required to provide ISPs monthly with the list of the individuals that connected to the internet using their network. The data should be stored locally for a period of at least six months. Later in 2015, the authorities proposed the following levels of fines for non-compliance: - 5,000-50,000 rubles (approx. 60-140 USD) for individual entrepreneurs; and - 100,000-200,000 rubles (approx. 1,400-2,600 USD) for legal entities. The fines would be higher for repeat offenders.	Multiple data types[167]	Across all sectors	Active
	5. According to the **Federal Law no. 152-FZ "On Personal Data" (OPD-Law)** the transfer of data outside Russia does not require additional consent from the data subject only if the jurisdiction that the personal data is transferred to ensures adequate protection of personal data. Those jurisdictions are parties to the Convention 108 and other countries approved by the Russian Federal Service for Supervision in the sphere of Telecom, Information Technologies and Mass Communications (Roskomnadzor). Roskomnadzor's official list of countries includes Australia, Argentina, Canada, Israel, Mexico and New Zealand.	Personal Data		Active

167. https://www.tanaza.com/blog/the-growth-of-public-wi-fi-in-russia/

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Russia	**6.** Russia's data localization legislation is officially known as Federal Law No. 242-FZ. It requires all domestic and foreign companies to accumulate, store, and process personal information of Russian citizens on servers physically located within Russian borders. Any organization that stores the information of Russian nationals, whether customers or social media users, must move that data to Russian servers.[168]	Personal Data		Active
	7. Federal Law No 374-FZ, signed in July 2016, requires local storage of information confirming the fact of receipt, transmission, delivery and/or processing of voice data, text messages, pictures, sounds, video or other communications (i.e., metadata reflecting these communications). The storage period is of three years (with respect to telecom providers) or one year (with respect to ISPs and message exchange services). In addition, local storage for a period of six months is required for the content of communications, including voice data, text messages, pictures, sounds, video or other communications. While the first requirement entered into force in July 2016, the second requirement came into force starting from July 2018.[169]	Personal Data and Metadata		Active
South Korea	**1. Act on the Establishment, Management, etc. of Spatial Data - Article 16** imposes a prohibition to store high resolution imagery and related mapping data outside the country and justifies this restriction on security grounds. It is reported that the prohibition led to a competitive disadvantage for international online map services, since their locally-based competitors are able to provide several services (such as turn-byturn driving/walking instructions, live traffic updates, interior building maps) that international service providers cannot.	Image and Mapping (Location and Spatial) Data[170]	Specific Sector	Active

168. https://www.bbc.com/news/technology-28583669
169. http://www.loc.gov/law/foreign-news/article/russia-new-electronic-surveillance-rules/
170 https://jsis.washington.edu/news/south-korean-data-localization-shaped-conflict/

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
South Korea	**2. The Personal Information Protection Act (PIPA)** enacted effective as of 30 September 2011, requires companies to obtain consent from data subjects prior to exporting their personal data. The legislative bills for the amendment of Personal Information Protection Act ("**PIPA**") are still pending at the National Assembly. Some of the key provisions in these bills include: (a) introduction of the concept of "anonymized" personal information, for the purpose of allowing the use anonymized personal information for commercial or research purposes; (b) permitting the collection and use of personal information without the consent of the data subject when the data subject has publicly disclosed his/her personal information; and (c) limiting the scope of "personal information" by limiting the scope of information that may be combined with other personal information to be used to "identify" an individual.[171]	Personal Data	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.

171. https://www.lexology.com/library/detail.aspx?g=fa96ac52-003b-4ec9-92b0-22fd0e8c1192

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
South Korea	**3. Act on Promotion of Information and Communications Network Utilisation (the Network Act):** If a user's personal information is transferred to an overseas entity, the Network Act requires online service providers to disclose and obtain the user's consent, regarding the following: the specific information to be transferred overseas, the destination country, the date, time, and method of transmission, the name of the third party and the contact information of the person in charge of the personal information held by the third party, the third party's purpose of use of the personal information and the period of retention and use. This act has been recently amended. Passed on August 30, 2018, amendment to the Network Act will require certain offshore information communication service providers which do not have an address or place of business in Korea, to appoint a local representative responsible for Korean data privacy compliance. This amendment will come into effect on **March 19, 2019**.[172,173]	Personal Data	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.

172. https://www.lexology.com/library/detail.aspx?g=fa96ac52-003b-4ec9-92b0-22fd0e8c1192
173. https://news.bloomberglaw.com/privacy-and-data-security/south-korea-privacy-law-changes-may-help-eu-data-transfer-talks

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
South Korea	**4. Financial Holding Company Act (FHCA):** Despite provisions in its FTAs with EU and US to allow financial data to be sent across borders, Korea prohibited outsourcing of data-processing activities to third parties in the financial services industry for several years and today certain restrictions still apply. Banks can therefore only process financial information related to Korean customers in-house, either in Korea or abroad and offshore outsourcing is restricted to a financial firm's head office, branch or affiliates. In June 2015, the Korea Financial Services Commission proposed revisions to its outsourcing policies by eliminating its requirements for (1) prior approval for the outsourcing of IT facilities; (2) offshore outsourcing to be restricted to a financial firm's head office, branch or affiliates (thus permitting use of third parties); and (3) use of a standardized outsourcing contract form (thus permitting customized contracts provided they include certain obligatory terms). Such revisions were implemented in July 2015. Yet, certain conditions for processing abroad still apply today.	Financial Data	Specific Sector	Active. The law is in force, however, data need not be localised under specific conditions.
Sweden	**1.** According to Swedish Accounting Act (Bokföringslag (1999:1078)), documents such as a company's annual reports, balance sheets and annual financial reports must be physically stored in Sweden for a period of seven years.	Company Records	Across all sectors	Active
	2. In relation to specific government authorities, there are certain provisions which might require the data processed by the authority to be held within Sweden or within the authority. This might affect the supply of cloud computing to public authorities.	Government Data	Across all sectors	Active

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Sweden	**3.** The Financial Services Authority requires 'immediate' access to data in its market supervision which, according to business, the supervisory body interprets as being given physical access to servers. Accordingly, Swedish financial services providers are de facto required to maintain all their records inside Swedish jurisdiction.	Financial Data	Specific Sectors	Active
	4. Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. The Data Protection Act (2018:218) and the Data Protection Ordinance (2018:19) (the "DPA") - The DPA regulates general aspects of data protection where the GDPR allows, e.g. processing of social security numbers and processing of data pertaining to criminal offences. The DPA entered into force on 25 May 2018.	Personal and Non-Personal data	Across all sectors	Active

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Sweden	**5.** In addition to the Swedish DPA, a vast number of sector specific acts have been adopted in Sweden, for example relating to the sectors of healthcare, finance, energy, environment, education, referendums/elections, enterprise, communication, labour market, etc. On 4 April 2018 in a draft to a proposal to the Council on legislation relating to personal data for scientific research purposes, the Swedish government criticised the proposal for a new scientific research data act, meaning that an update of other acts (such as the Ethical Review Act) will be enough in order to complement the GDPR. As a result of this the Swedish parliament in November 2018 voted in favor of the proposed amendments to acts relating to the processing of personal data for scientific research purposes, which did not include the adoption of a new scientific research data act. The amendments to the relevant acts entered into force on 1 January 2019.	Personal Data[174] for various sectors		Active
Taiwan	**1.** Under the Personal Data Protection Act (PDPA), the transfer of personal information to mainland China is prohibited	Personal Data	Across all sectors	Active
	2. There is no consent requirement for transfer in third countries, but the data subject has to be notified in advance that his/her personal data is being transferred to another country. Yet, according to Article 21 of the Personal Data Protection Act (PDPA), the international transmission of personal information can be interrupted by the central competent government authority if the transmission involves major national interests or if the country receiving personal information lacks adequate data protection laws.	Personal Data	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.

174. https://www.dlapiperdataprotection.com/index.html?t=law&c=SE&c2=

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Taiwan	**3.** The Financial Supervisory Commission (FSC) established stringent rules for processing of personal financial information off-shore. Yet, on May 2014, the requirements that both local and foreign banks establish standalone onshore data centres were lifted.	Financial Data	Specific Sector	Discontinued
Turkey	**1.** Article 23 of Law No. 6493 requires that "the system operator, payment institution and electronic money institution shall be required to keep all the documents and records related to the matters within the scope of this Law for at least ten years within the country, in a secure and accessible manner". The article also specifies that "the information systems and their substitutes, which are used by system operator to carry out its activities shall also be kept within the country".	Financial Data	Specific Sector	Active
	2. The Data Protection Law/The Law on Protection of Personal Data No. 6698 (LPPD) which is based on EU Directive 95/46/EC[175] stipulates that data cannot be processed or transferred abroad without the individual's explicit consent. Consent will not be required if the transfer is necessary to exercise a right or is required by law, and either: - Sufficient protection exists in the transferee country, or - if the data controller gives a written security undertaking and Turkey's Data Protection Board grants permission.	Personal data	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.
	3. According to the Electronic Communication Act, the transfer of traffic and location data abroad is permitted with the data subjects' explicit consent.	Personal data	Across all sectors	Active

175. https://www.dlapiperdataprotection.com/index.html?t=law&c=TR

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Turkey	**4.** There exist several regulations that try to implement various facets of LPPD. The important ones are mentioned below:[176] • Regulation on the Erasure, Destruction and Anonymizing of Personal Data (published in the Official Gazette dated October 28, 2017, numbered 30224) • Regulation on the Working Procedures and Principles of Personal Data Protection Board (published in the Official Gazette dated November 16, 2017, numbered 30242) • Regulation on the Registry of Data Controllers (published in the Official Gazette dated December 30, 2017, numbered 30286) • Regulation on the Organization of Personal Data Protection Authority (published in the Official Gazette dated April 26, 2018, numbered 30403) • The Communiqué on Procedures and Principles for Compliance with the Obligation to Inform (published in the Official Gazette dated March 10, 2018, numbered 30356) • The Decision of Data Protection Board, dated January 31, 2018, numbered 2018/10 on Adequate Measures to be taken by Data Controllers in Processing the Special Categories of Personal Data	Personal Data		Active
United Kingdom	According to the Companies Act 2006, "if accounting records are kept at a place outside the United Kingdom, accounts and returns (...) must be sent to, and kept at, a place in the United Kingdom, and must at all times be open to such inspection".	Company Records	Specific sectors	Active

176. https://www.dlapiperdataprotection.com/index.html?t=law&c=TR&c2=

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
United Kingdom	Alongside the GDPR, the United Kingdom has prepared a new national data protection law, the Data Protection Act 2018 ("DPA"), which came into force on 25 May 2018. As well as containing derogations and exemptions from the position under the GDPR in certain permitted areas, the DPA also does the following: • allows for the continued application of the GDPR in UK national law once the UK leaves the European Union (expected to be 29 March 2019); Part 3 of the DPA transposes the Law • Enforcement Directive ((EU) 2016/680) into UK law, creating a data protection regime specifically for law enforcement personal data processing; Part 4 of the DPA updates the data • protection regime for national security processing; and Parts 5 and 6 set out the scope of the • Information Commissioner's mandate and her enforcement powers, and creates a number of criminal offences relating to personal data processing.	Personal Data[177]		Active
	Two sets of regulations, **The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019** and The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) (No. 2) Regulations 2019 have been promulgated which were made pursuant to the EU (Withdrawal) Act 2018 (EUWA). These will come into force upon UK's withdrawal from EU. Broadly speaking, these regulations are intended to preserve the status quo post-Brexit by (1) amending certain provisions of the GDPR to allow it to be retained as UK domestic law and (2) transitionally adopting certain key decisions of the EU institutions that, collectively, would allow for the continued lawfulness of personal data flows out of the United Kingdom where currently permitted under EU law			Inactive currently

177. https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/about-the-dpa-2018/

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Vietnam	**1.** The Decree No. 72/2013/ND-CP of July 15, 2013, on the Management, Provision and Use of Internet Services and Online Information entered into force in September 2013 establishes local server requirements for online social networks, general information websites, mobile telecoms network based content services and online games services. All these organisations are required to establish at least one server inside the country "serving the inspection, storage, and provision of information at the request of competent state management agencies". The Government of Vietnam recently issued Decree No. 27/2018/ND-CP ("Decree No. 27") to amend and supplement Decree No. 72/2013/ND-CP dated 15 July 2013 on the management, provision, and use of Internet services and online information ("Decree No. 72"). Decree No. 27 took effect on 15 April 2018. Aggregated information websites and social networks are required to set up a warning mechanism in case their members post illegal content (filter). In the event of illegal content being posted on their platforms, aggregated information websites and social networks must have a coordinating mechanism to remove illegal content within three (3) hours after the aggregated information websites and social networks discover such illegal content or receive takedown requests from the MIC or licensing authorities via written documents, telephone or email.[178]	Multiple data types	Across all sectors	Active
	2. According to the Decree 90 of 2008, advertising service providers that use email advertisements and internet based text messages are required to send emails from a Vietnamese domain name (".vn") website which is operated from a server located in Vietnam.	Domain Data[179]	Specific sectors	Active

178. https://www.lexology.com/library/detail.aspx?g=bec72ba6-167d-468e-938c-391199d8579c
179. https://luatminhkhue.vn/en/decree-no-90-2008-nd-cp-dated-august-13--2008-of-the-government-against-spam.aspx

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Vietnam	**3.** On June 12, 2018, the Vietnamese National Assembly passed the Law on Cybersecurity (the "Cybersecurity Law"), which was enforced on January 1, 2019. Among other aims, the law seeks to regulate data processing methods of technology companies that operate in Vietnam and restrict the internet connections of users who post "prohibited" content. The Cybersecurity Law will, in principle, affect both domestic and foreign companies that provide services through telecommunication networks or the internet, or value-added services to customers in Vietnam. Interpreted broadly, these services would include social networks, search engines, online advertising, online broadcasting and streaming, e-commerce websites and marketplaces, internet-based voice/text services (OTT services), cloud services, online games and other online applications. The Cybersecurity Law will be required to store the personal data of Vietnamese end-users in Vietnam for the legally prescribed period of time, and surrender such data to Vietnamese government authorities upon request. Foreign companies providing telecommunications or internet services in Vietnam must:[180, 181, 182] • Establish offices in Vietnam • Store the personal information of Vietnamese users and "other important data" in Vietnam and perform a security assessment prior to any cross-border data transfer; • Bring their technology products involving cyber services into compliance with "quality assurance" standards before they can be released to the market.	Multiple data types	Specific sectors	Active

180. http://www.mondaq.com/x/712298/Data+Protection+Privacy/Vietnam+Passes+Sweeping+Cybersecurity+Law
181. https://thediplomat.com/2019/01/vietnams-controversial-cybersecurity-law-spells-tough-times-for-activists/
182. https://www.straitstimes.com/asia/vietnams-cyber-security-law-takes-effect-amid-criticism

Country	Measures to Regulate Cross-Border Flow of Data	Scope of Data Types	Scope of Sectors Affected	Status
Vietnam	It also requires administrators of information systems critical to national security to store personal data and "critical data" within the national territory of Vietnam. It is unclear when an information system develops to a point that it is critical to national security. Neither is it clear whether the systems cover state-owned systems only or include private systems as well. "Critical data" is also not defined.[183]			

Source – Compiled by authors using data from ITIF, ECIPE, DLA Piper and other secondary sources

183. https://ecipe.org/dte/database/page/7/?country&chapter=829&subchapter=830

Table A1.2: Data Regulation Measures in India

Measure of Data Regulation	Process of Design and Implementation	Status (Active/ Proposed)
Draft E-Commerce Policy, 2019[184]	The first draft was circulated in 2018 and retracted after strong opposition from stakeholders. Another version of the draft policy has been circulated in 2019. The policy was open for stakeholder comments and a stakeholder consultation was also held.	Proposed
The Draft Personal Data Protection Bill, 2018[185]	The draft was open for public comments. The final draft will be presented to the Ministry of Electronics and Information Technology for consultation which might lead to further amendments before it is introduced in the Parliament.	Proposed
RBI Notification on 'Storage of Payment System Data'[186], 2018	The directive was notified without any prior consultation as well as any explanations behind its motivations. Stakeholders have raised concerns over lack of clarity in the guidelines.	Active
Draft E-Pharmacy Regulations, 2018 (Amendment to Drugs and Cosmetics Rules, 1945)[187]	The draft was circulated in August 2018 and a period of 45 days was assigned for stakeholder comments. A final version of the policy has not yet been released.	Proposed
FDI Policy, 2017[188] (localisation requirement only for companies in the broadcasting sector)	Changes were made to the earlier FDI policy after intensive consultations with stakeholders including apex industry chambers, associations, industry bodies etc. and their views/ comments were taken into consideration.[189]	Active

184 https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf
185 https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf
186 https://rbidocs.rbi.org.in/rdocs/notification/PDFs/153PAYMENTEC233862ECC4424893C558DB75B3E2BC.PDF
187 https://www.medianama.com/wp-content/uploads/1890431.pdf
188 https://dipp.gov.in/sites/default/files/CFPC_2017_FINAL_RELEASED_28.8.17_0.pdf
189 http://pib.nic.in/newsite/PrintRelease.aspx?relid=158262

Measure of Data Regulation	Process of Design and Implementation	Status (Active/ Proposed)
National Telecom M2M Roadmap, 2015[190]	For certain issues related to the roadmap, TRAI's recommendations were sought, for which TRAI floated a consultation paper which was open to stakeholder comments.	Active
Unified Access License for Telecom, 2004[191]	The first guidelines were announced in 2003 and a consultation paper was floated by the TRAI for stakeholder comments. Further another consultation paper was floated in 2004. Subsequent amendments to the guidelines have been enforced after due consideration of stakeholder comments.	Active
Companies Act, 2013 and Rules (Companies Accounts Rules, 2014)[192]	After the Companies Bill, 2013 was passed, its rules were made open for stakeholder comments. For the Companies Accounts Rules, 2014, recommendations were sought from the National Advisory Committee on Accounting Standards.	Active
IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017[193]	A proposed draft was circulated in 2016 which invited comments from stakeholders.	Active

190 http://dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf
191 http://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf
192 http://www.mca.gov.in/Ministry/pdf/NCARules_Chapter9.pdf
193 https://taxguru.in/wp-content/uploads/2017/01/Proposed-IRDAI-Outsourcing-of-Activities-by-Indian-Insurers-Regulations-2017.pdf; https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_NoYearList.aspx?DF=RL&mid=4.2

Measure of Data Regulation	Process of Design and Implementation	Status (Active/ Proposed)
Guidelines on Contractual Terms Related to Cloud Services under the MeghRaj Initiative, 2017[194]	The DoT sought recommendations from the TRAI on licensing and regulatory issues arising from cloud services. TRAI issued a consultation paper in 2016. The TRAI received comments from stakeholders and also conducted an Open House Discussion with stakeholders in 2017. The Authority then released its recommendations based on stakeholder comments and discussions.	Active
Information Technology Act, 2000 and Rules[195]; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (IT Rules)[196]	Comments on the 2011 rules were submitted by stakeholders to the Committee on Subordinate Legislation. The Committee then submitted a report based on the submissions received to the Lok Sabha.	Active
Public Records Act, 1997[198]	Not available	Active
SEBI Data Privacy Rules for Foreign Portfolio Investors (in process)[199]	SEBI is currently working on the data privacy norms for FPIs.[200]	Proposed
National Cloud Computing Policy (in process)	TRAI floated a consultation paper on cloud computing and several stakeholders have submitted their comments.[201] The panel working on the policy wants data to be stored within the country according to its draft report. policy wants data to be stored within the country according to its draft report.[202]	Proposed

Source – Compiled by authors

194 https://www.meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf
195 https://meity.gov.in/writereaddata/files/itbill2000.pdf; https://meity.gov.in/writereaddata/files/act2000_0.pdf
196 https://meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf
197 https://www.prsindia.org/uploads/media/IT%20Rules/IT%20Rules%20Subordinate%20committee%20Report.pdf
198 http://nationalarchives.nic.in/sites/default/files/public.pdf
199 https://www.sebi.gov.in/legal/regulations/jan-2019/sebi-foreign-portfolio-investors-regulations-2014-last-amended-on-december-31-2018-_41702.html
200 https://www.cmie.com/kommon/bin/sr.php?kall=warticle&dt=2019-01-08%2012:05:45&msec=446&ver=pf
201 https://main.trai.gov.in/sites/default/files/Cloud_Computing_Consultation_paper_10_june_2016.pdf
202 https://in.reuters.com/article/us-india-data-localisation-exclusive/exclusive-india-panel-wants-localization-of-cloud-storage-data-in-possible-blow-to-big-tech-firms-idINKBN1KP08J

Appendix 2

Table A2.1 : Literature Review – Impact of ICT on International Trade

Title of Study	Authors	Methodology	Findings
The effect of the internet on International Trade (2004)	C. Freund and D. Weinhol	Sample of 56 developed and middle income countries for the period 1995 – 1999. Number of website domain names in every country is used as the measure of internet. They use panel growth regressions and cross sectional traditional gravity estimation.	10% increase in the growth of internet users leads to a 1% increase in exports.
Communication costs and Trade of Differentiated Goods (2006)	L. Tang	Investigates how the proliferation of communication technologies impact US imports of differentiated and homogenous goods. Data from 1975 – 2000 is used and the author contrasts the impact of exporting country adoption of fixed line telephones, mobile phones and the number of computers connected to the internet. The model uses time fixed effects.	All measures of technology have a positive and significant impact on US imports of differentiated goods, but not those sold on organised exchange. A 10% increase in the internet connections of the exporter leads to an increase in US imports of differentiated goods by approximately 1%.
Impact of Commercialization of the internet on International Trade: A Panel Study Using the Extended Gravity Model (2009)	V. K. Vemuri and S. Siddiqui	The minimum of exporter and importer adoption of the internet is taken as a measure of internet proliferation. Unobserved bilateral factors are controlled for.	A 10% increase in internet adoption leads to a 2% increase in bilateral trade.
Has the internet increased trade? Developed and Developing country evidence (2006)	G. Clark and S. Wallsten	Uses cross-section of 101 countries in 2001. They use an instrumental variable approach where the instrument used is internet hosts with data on the level of competition in the telecommunications sector. They use this to investigate the potential differential impact of the internet on trade within and between developed and developing countries.	internet penetration leads to an increase in exports from developing to developed countries, but does not impact any other trade flow. They also find that improving internet access can boost a developing country's exports to high-income economies. Their instrumental variable also implies suggests that regulatory policies in developing countries that restrict telecommunications and internet development also indirectly restrict exports.

Title of Study	Authors	Methodology	Findings
Does the internet defy the Law of Gravity? (2006)	B. Blum and A. Goldfarb	Uses a gravity model to estimate the consumption of digital goods over the internet.	Distance plays an important role in determining the websites visited by households although there are no direct transportation costs involved. The authors find that preferences play an important role in determining the geography of trade patterns.
Assessing the impact of communication costs on international trade (2005)	C. Fink, A. Mattoo, I.C. Neagu	Authors introduce communication costs into a gravity model of trade measured using cost of an international telephone between the exporting and importing countries. This limits the data to a cross-section in 1999. They also instrument telephone costs with measures of competition in the telecommunication sector in each country. They also control for importer and exporter fixed effects.	A 50% decrease in importers' calling price leads to a 42.5% increase in trade.
Goods Follow Bytes: The Impact of ICT on EU Trade (2012)	A.Mattes, P. Meinen and F. Pavel	Authors construct a dummy variable composite index that combine measures of the internet, broadband, mobile phones and education levels for EU countries for the period 1995 – 2007. Time varying country specific effects are also controlled for.	Countries with an ICT index above the mean have 52% higher bilateral trade than those with an ICT index below the mean.
The internet and International Trade in Goods (2012)	J. Timmis	A panel of OECD countries for the period 1990 to 2010 is used. The author uses a fixed effects approach to control for multilateral resistance and unobservable factors.	Country pairs with relatively higher adoption rates of the internet trade more with one another than country pairs with lower adoption rates. But the author does not find significant evidence of the effect of increase in internet adoption within country pairs, on trade.

Source – Compiled by authors from Timmis (2012), Vemuri and Siddiqui (2009) and Clark and Wallsten (2006)

Table A2.2: Literature Review : Impact of Data and Data Localisation

Study	Author (s)	Methodology	Estimates
Quantifying the Cost of Forced Data Localisation (2015)	Leviathan Security Group	Compares cloud services with the most equivalent offerings by equating cloud instances based on memory allocated to each instance, which is directly correlated to CPU resources on each platform	Local companies would be required to pay 30-60% more for their computing needs if there is a forced data localisation legislation
Digital Trade in the U.S and Global Economies (2014)	United States International Trade Commission	Survey of approximately 10,000 U.S firms using stratified random sampling approach and. The data is then used in an econometric model with a logit functional form that estimates each firm's estimate of productivity effects to its use of the internet	Removing foreign digital trade barriers would increase U.S GDP by 0.1-0.3% and wages by 0.7-0.14% in digitally intensive sectors. Digital trade raised GDP in the US by 3.4-4.8% and contributed to creating 2.4 million new jobs
Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localisation (2016)	Matthias Bauer, Martina F. Ferracane and Erik Van Der Marel	A regulatory data index developed using the input-output model is used as the independent variable to study the Total Factor Productivity and a price index based on value added calculations for a set of countries using standard parametric estimation techniques. The law proposals are quantified and an index developed which is then used to calculate TFP losses in the counterfactual situation where countries implement the proposed regulatory laws on data	Data localisation and commonly used barriers to data flows decreased TFP, which further reduced GDP by 0.1% in Brazil, 0.55% in China, 0.48% in the EU and 0.58% in South Korea

Study	Author (s)	Methodology	Estimates
The Costs of Data Localisation: Friendly Fire on Economic Recovery (2014)	Matthias Bauer, Hosuk Lee-Makiyama, Erik Van Der Marel and Bert Verschelde	Develops a regulatory data index (DRL) for the selected countries and then extends it to the sectoral level using data intensities in each sector. The GTAP model is used to estimate the macroeconomic impact of movements in TFP as a result of changes in data regulation policies	The impact of proposed or enacted data restrictions on GDP – Brazil (-0.2%), China (-1.1%), EU (-0.4%), India (-0.1%), Indonesia (-0.5%), Korea (-0.4%) and Vietnam (-1.7%). With economy wide data localisation requirements, the impact would be – Brazil (-0.8%), EU (-1.1%), India (-0.8%), Indonesia (-0.7%) and Korea (-1.1%). There are also negative impacts on investments and losses to consumer welfare from data localisation policies
The Economic Impact of Getting Data Protection Right (2013)	Matthias Bauer, Fredrik Erixon, Michal Krol, Hosuk Lee-Makiyama, assisted by Bert Verschelde	GTAP 8, a computational general equilibrium model is used. The regression uses firm-level costs translated into restrictiveness applied to production or cross border trade and other ad-valorem equivalents that are tariff or tax equivalents on economic activities	GDPR leads to a decline in EU's service exports to the US by 6.7%. US service exports to the EU decrease by 16.6-24% and exports from other countries to the EU fall by up to 80%. The GDPR decreases EU GDP by 0.8-1.3%. EU's manufacturing exports to the US estimated to decrease by up to 11%.
Unleashing Internal Data Flows in the EU: An economic Assessment of Data Localisation Measures in the EU member states (2016)	Matthias Bauer, Martina F. Ferracanne, Hosuk-Lee Makiyama and Erik Van Der Marel	GTAP 8, a computational general equilibrium model is used. It allows for a general equilibrium analysis of the economic effects of the regulation of cross-border data flows	Best case scenario – removal of existing data localisation policies would increase the GDP of individual EU member economies by 0.05% in the UK and Sweden, 0.06% in Finland, 0.07% in Germany, 0.18% in Belgium and 1.1% in Luxembourg. Worst case scenario – Full data localisation policies would remove 0.4% from the EU economy each year ranging from -0.27% in Croatia to -0.61% in Luxembourg. The loss in output in the ICT sector ranges from 0.54% in Poland to 3.46% in Luxembourg.

Study	Author (s)	Methodology	Estimates
Economic Impact of Data Localisation in Five Selected African Countries (2018)	Mona Farid Badran	Develops a regulatory data index (DRL) for the selected countries and then extends it to the sectoral level using data intensities in each sector. The GTAP model is used to estimate the macroeconomic impact of movements in TFP as a result of changes in data regulation policies	The estimated elasticity for the five countries (Mauritius, South Africa, Egypt, Morocco and Kenya) is 0.347 which is much lesser than the elasticity in the set of EU countries examined in the paper, thus showing that the impact of data localisation on TFP was lower in these five countries than in the more advanced EU economies.
Digital Globalization: The New Era of Global Flows (2016)	James Manyika, Susan Lund, Jacques Bughin, Jonathan Woetzel, Kalin Stamenov, Dhruv Dhingra	The model is based on a Cobb-Douglas production function and a two-step error correction model is used, in order to test for the additional effect of cross border data flows on GDP growth, in addition to capital and labour	Global flows have raised world GDP by 10% over the last decade. The GDP increase from data flows has been $2.8 trillion. For some countries there could be a 50% potential GDP boost from increased participation in global flows
The Impact of Data Protection Regulation in the EU (2013)	Christensen, Colciago, Etro, Rafert	Evaluates the impact of the then proposed EU Data Protection Regulations on SMEs with a specific focus on job growth and business creation. The methodology is as follows ; a) Selected articles from the Regulation and estimated direct costs to be incurred by SMEs using the EC Impact Assessment and third party verifications b) Estimated the average annual increase in cost for an average SME by sector Simulated the impact of increased costs on business and job creation using DYNARE's dynamic stochastic general equilibrium model	Estimated that the annual average increase in costs for an SME in EU would be in the range of 3000 to 7200 Euro and would vary by sector. This estimate represents 16% to 40% of the current annual SME IT budget. The Regulations will have a substantial negative impact on business and job creation. Real Estate and Business Activities sector is likely to experience a decline in employment of between 0.2 and 0.6 percent and in the number of market competitors between 3 and 5 percent

Study	Author (s)	Methodology	Estimates
A Methodology to estimate the costs of data regulations (2015)	Erik Van der Marel, Matthias Bauer, Hosuk Lee-Makiyama and Bert Verschelde	Explores how data regulation is systematically related to the performance of downstream manufacturing and service industries in a typical economy. The methodology is as follows ; Develops a regulatory data index that serves as a proxy indicator for regulation in data. Augment the index to assess whether the regulations impact downstream industries. Measure the impact of data regulations on Total Factor Productivity. The results of this exercise are used in a CGE model to estimate the macroeconomic feedback effects across the wider world economy	The results suggest that administrative regulatory barriers in sectors using data processing services most intensively exhibit a dampening effect on TFP and an upward pressure on prices. The simulation results from the CGE model finds that restrictions on free flow of data negatively impact economic activity in the medium –long term. The production of data-intensive manufacturing and services sectors shrink in all countries.
Data As a Driver of Economic Efficiency (2018)	Jia and Wagman (Data Catalyst)	Analyses the consequence of data regulation on investment, consumer prices and overall economic welfare. The paper uses two policy events – EU's General Data Protection Regulation and privacy ordinances in the San Francisco Metropolitan Statistical Area. Collects and analyses data on venture fund activity in the technology sector for EU and US during the period July 2017 and September 2018. Contrast venture fund activity in the EU and US before and after the rollout of GDPR and test the effect of the enactment of GDPR using a difference –in-difference methodology.	The findings indicate a significant negative differential effect on EU ventures after GDPR came into effect relative to their US counterparts. However, the long term consequences of GDPR on venture funding for EU technology companies will be clear once more data is available over time

Study	Author (s)	Methodology	Estimates
Quantifying the Cost of Forced Localisation (2015)	Leviathan Security Group	Measures the cost of forced data localisation. The paper collects data on the typical rate of "Infrastructure as a Service" (IaaS) cloud computing providers across countries and estimates the cost implications when users are forced to use domestic servers versus international options across a set of 7 cloud service providers	Since the cloud data centers were distributed across a very small number of countries , forced localisation laws would severely impact countries such as Canada, India, Indonesia and Russia, which would be restricted to choosing from domestic service providers vis-à-vis the advantages of accessing services of global operators. For example, in Brazil, ,a customer would have to pay 54.65% less if permitted to use cloud services outside Brazil

Source – Compiled by authors

Appendix 3

Table A3.1: Results from Econometric Estimation

Variable	Coefficient	Standard Error	p – Value
L1.logX$_{ij}$	1.46	0.27	0.00
logYPCdif$_{ij}$	9435.97	4259.08	0.03
logRER$_{ij}$	1423.40	710.13	0.05
logIIB$_{ij}$	696.71	348.47	0.05
logDistance$_{ij}$	-23254.43	9915.569	0.02

Source: Authors' calculations

Appendix 4

Table A4.1: Summary of Case Studies

Name of Organisation	Type of Organisation	Year of Incorporation	No. of Employees	Company Origin/ Headquarters	Country/ Countries of Operation
Financial Services 2	Private	2015	51 - 200	India	India
Financial Services 1	Private	2014	51 - 200	Singapore	Global
Travel and Hospitality	Private	2000	3051	India	Global

Sector of Operation	Data Storage	Cross-border Data Flow	Data Localisation in India	Data Localisation in Other Countries	Impact/ Potential Impact of Data Localisation in India
Financial Services	All data stored in cloud using services provided by AWS. Data was relocated to Indian servers in Mumbai by AWS.	No	Compliant as all data is stored in servers in India	Not applicable.	No impact as all data is stored in India.
Financial Services	They use own data servers in India. In other countries, they use either own data servers or cloud services	Yes	All data related to Indian customers stored in India, and therefore compliant.	Compliant with data regulations in other countries of operation. Compliant with GDPR	No impact as data of Indian customers and transactions are already stored in India. In the absence of data localisation requirements, they would have preferred hosting data on cloud services overseas.
Travel and Hospitality	They have two data centres in India, in Chennai and Mumbai, but they are in the process of migrating their data to AWS in Mumbai.	Yes	All data stored in India, therefore, compliant. All data is anonymised and is part of internal compliance.	Take consent to store data of EU customers and offer the option of opting out. All data is anonymised and is part of internal compliance.	No impact as all data is stored in India.

Name of Organisation	Type of Organisation	Year of Incorporation	No. of Employees	Company Origin/ Headquarters	Country/ Countries of Operation
Financial Services 6	Private	1966	Above 10,000	United States of America	Global
Financial Services 3	Private	2011	51 - 200	India	Global

Sector of Operation	Data Storage	Cross-border Data Flow	Data Localisation in India	Data Localisation in Other Countries	Impact/ Potential Impact of Data Localisation in India
Financial Services	Data stored in global data servers located outside India. As of October 2018, all data related to Indian transactions is being stored in their technology centre in Pune.	Yes	Compliant with RBI guidelines as of October 2018.	Compliant with GDPR.	Direct impact on value added services. There can be a break down in the charge back system. The fraud detection system can be affected. Impacts loyalty services and has a bearing on Indian card holders and also affects foreign consumers coming to India. Overall, it will weaken safety and security over a period of time.
Financial Services	Data stored on cloud. It uses cloud services provided by Google and based in Mumbai. All personally identifiable data is purged. Metadata is used.	No	No personally identifiable data is stored. Metadata is hosted on cloud in India.	Compliant with GDPR.	No impact.

Name of Organisation	Type of Organisation	Year of Incorporation	No. of Employees	Company Origin/ Headquarters	Country/ Countries of Operation
Financial Services 4	Private	2017	2 - 10	India	India
Social Networking	Private	2015	11 - 50	India	India
Health and Technology (Social Enterprise)	Private	2002	100	United States of America	Global

Sector of Operation	Data Storage	Cross-border Data Flow	Data Localisation in India	Data Localisation in Other Countries	Impact/ Potential Impact of Data Localisation in India
Financial Services	They store personally identifiable data like e-mail address, name, name of bank account, UPI of bank account, in addition to IP address and browser details etc. Data is stored on cloud, using services provided by AWS. They take users' consent to use their data for analytics, measuring activity on their website etc.	No	Compliant as all data is stored in India.	Its privacy policy is very closely compliant with GDPR, but it is not operational outside India.	No impact.
Social Networking	All data stored on cloud in India, using services provided by AWS.	No	Compliant as all data is stored in India.	Not applicable	No impact.
Social Enterprise (Health and Technology)	They had two data servers – one in India and another in USA. In India, they initially used their own servers, then used servers provided by NIC as they implemented government projects. They now use cloud services provided by a private organisation. All data for projects in South-East Asia is stored in India and the rest is stored in the USA.	No	They are compliant because they work on development projects for the government for which data localisation is a pre-requisite.	It is certified and complies with the EU-US and the Swiss-US Privacy Shield Programs.	Storing data on server space provided by NIC led to inefficiencies. It would be operationally easier for them to manage data stored in the US server. In India, the government is willing to maintain data localisation at the cost of delaying projects.

Name of Organisation	Type of Organisation	Year of Incorporation	No. of Employees	Company Origin/ Headquarters	Country/ Countries of Operation
Communications	Private	2009	51 - 200	Europe	Global
Financial Services 5	Private	2014	201 - 500	India	India

Sector of Operation	Data Storage	Cross-border Data Flow	Data Localisation in India	Data Localisation in Other Countries	Impact/ Potential Impact of Data Localisation in India
Social Networking	All data is classified into EU and non-EU data. All EU data is stored in EU and the non-EU data is stored in India. They have a data centre in Europe. Data in India is stored on cloud using services provided by Google. They do not store any sensitive data such as credit card or bank information. All payments related data stored at the backend and managed by a public sector and a private sector bank.	Yes	Compliant as data of Indian customers is locally stored.	Compliant with GDPR.	No significant impact.
Financial Services	Data stored on cloud using services provided by AWS. Earlier data was stored in servers in Singapore, but they had to migrate to servers in Mumbai. A second copy of the data is stored in Singapore. They collect sensitive information of users.	No	Compliant as data is stored in servers located in India.	Not applicable.	Incurred costs to migrate data from servers in Singapore to servers in India. Additionally there were time costs and other overheads.

Name of Organisation	Type of Organisation	Year of Incorporation	No. of Employees	Company Origin/ Headquarters	Country/ Countries of Operation
Digital Media	Private	1982	Above 10,000	United States of America	Global
Education	Private	2011	51 - 200	India	India
Financial Services 7	Private	2015	21,800	United States of America	Global
Food and Lifestyle	Private	2008	1001 - 5000	India	Global
Consumer Electronics	Private	1969	Above 10,000	South Korea	Global

Sector of Operation	Data Storage	Cross-border Data Flow	Data Localisation in India	Data Localisation in Other Countries	Impact/ Potential Impact of Data Localisation in India
Digital Media and Marketing	They host data on cloud, using services provided by Azure or Amazon. They choose between the two service providers depending upon the continent of operation.	Yes	No information available.	Compliant with GDPR.	Not directly affected by data localisation. However, GDPR compliance did impact them. The increased costs would eventually have to be passed on to the consumers.
Education	All data is hosted on cloud, using services provided by AWS in Singapore. (yet to confirm if they have migrated to the Mumbai centre)	No	No information available.	Does not comply with GDPR but provides an option to opt out of receiving e-mails.	No impact.
Financial Services	Data stored in cloud outside India.	Yes	Lack of clarity on RBI directive, therefore, status of compliance is ambiguous	Compliant with GDPR	High impact.
Consumer internet (Food and Lifestyle)	All data is hosted on cloud using services provided by AWS in Singapore.	Yes	Not yet applicable	Compliant	High impact.
Consumer Electronics (predominant vertical). Other verticals of operation include construction, payments, research and development etc.	All data is hosted on cloud. Details on location of cloud services not available.	Yes	Compliant with RBI's payment data localisation mandate	Compliant	High impact.

Source – Compiled by authors based on stakeholder interviews

Appendix 5

Table A5.1: Data Storage in Multiple Locations

Only in own servers (both in India and in other countries)	42
Only in India (both in own and outsourced servers)	18
Own servers in India and outsourced servers in other countries	0
Own servers in India and other countries and outsourced servers in India	17
Own servers in India and other countries, and outsourced servers in other countries	1
Own and outsourced servers in India, and outsourced servers in other countries	1
Own and outsourced servers in India and in other countries	2
Own servers in other countries and outsourced servers in India	4
Own and outsourced servers in other countries	2
Own and outsourced servers in other countries and outsourced servers in India	0
Outsourced servers in India and in other countries	1

Source: Authors' calculations from enterprise survey data

Appendix 6

Business Survey Questionnaire

Economics of Data Localisation

Survey on how businesses operating in India will be/ have been impacted by the proposed/ implemented measures of Data Localisation in India

Localisation norms in India have existed through different laws and policies, even before the Draft Personal Data Protection Bill, 2018[203]. For example, the Public Records Act, 1993, prohibits transfer of public records out of the country without prior approval of the Central Government. Similarly, the Companies (Account) Rules, 2014 state that the back-up of books of account and other books and papers of the company maintained in electronic mode, including at a place outside India, should be kept in servers physically located in India, on a periodic basis.

The discussion on data localisation was re-ignited with the Draft Personal Data Protection Bill, 2018. Sections 40 and 41 of the Bill[204] propose conditions for and restrictions on cross-border transfer of personal data; it requires a serving copy of all personal data be stored in India and that certain categories of 'critical personal data' - a subset of sensitive personal data, to be processed only in a server or data center in India, and that the Government will notify particular countries, sectors, or international organizations that may be exempt from restrictions on free flow of data across borders on the grounds of necessity or strategic interest of the state[205].

The Reserve Bank of India (RBI) recently noted that security measures were necessary for India's rapidly expanding digital payment ecosystem. As a part of its security measures, the RBI, in April 2018, issued a directive[206] that mandates (i) All system providers to store payment related data only in India and that (ii) System providers ensure compliance within six months and report compliance to the RBI by October 15, 2018. Furthermore, India's Draft National Policy Framework for E-Commerce in India also includes provisions for data localisation measures[207]. In May 2018, India's health ministry also proposed a law for protecting citizens' health data by granting them complete ownership of it.

The policies are likely to impact business processes that involve cross border flow of data as well as data processing and data storage within a jurisdiction. Through this survey, we seek inputs from businesses operating in India (whether or not they have an established physical presence in the country) for a better understanding of how an enterprise processes data and how the proposed / implemented data localisation measures are likely to impact them. Your feedback will improve the credibility of our analysis. Your responses will be kept strictly confidential. Thank you!

Please feel free to reach out to mkedia@icrier.res.in or gvarma@icrier.res.in for any queries

203 See Bailey and Parasheera (2017)
204 See: Draft Personal Data Protection Bill, 2018
205 See: Bailey, et.al, 2018, Comments on the (Draft) Personal Data Protection Bill, 2018
206 See: https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0
207 See: Electronic Commerce in India: Draft National Policy Framework, 2018

A. Company Profile

1a. Organisation type (Select One)

(i) Government/Public Sector

(ii) Private

(iii) Not for profit

1b. Sector of activity _____

(Use Sector Code)

2. Location of office _____

(Use City Code)

3. Year of Incorporation _____

4a. Does your company belong to another company or a group of companies?

(i) No

(ii) Yes, belong to a group as a subsidiary

(iii) Yes, controls a group of firms

4b. If the response to question 4a is (ii), where is the company headquartered?

_____ (Use Country Code)

4c. In how many different countries does your company have an operating office?

(i) 1

(ii) 2-5

(iii) 6-15

(iv) more than 15

5. What is the employee strength of your business

a) At your location _____

b) Total group of companies (if applicable) _____

6. What is the annual revenue of your company?

a) At your location _____

b) Total group of companies (if applicable) _____

If response to Q10 is (ii) No , please skip question 11

11a. Which are the top 3 countries to which you send/ from which you receive data (Use Country Code - If there are less than 3, leave some responses blank)

(i) _____

(ii) _____

(iii) _____

11b. Please select all activities which involve cross border flow of data (Select all that apply)

(i) Domestic Production/ Service Delivery
(ii) Domestic Client/ Customer Service
(iii) International Production/ Service Delivery
(iv) International Client / Customer Service
(v) Dealing with suppliers and vendors
(vi) Dealing with other subsidiaries (in case of a group company)
(vii) Marketing and Distribution
(viii) Personnel Management
(ix) Business Compliance
(x) Risk Management
(xi) Others. Please specify _____

11c. What percentage of the data flows across borders?

(i) None
(ii) Less than 10 percent
(iii) 10 – 30 percent
(iv) 30 – 50 percent
(v) 50 – 80 percent
(vi) Greater than 80 percent

11d. What percentage of the cross border data flow is likely to be personal data?

(i) None
(ii) Less than 10 percent
(iii) 10 – 30 percent
(iv) 30 – 50 percent
(v) 50 – 80 percent
(vi) Greater than 80 percent

I12. Does your company segregate between types of data? Select all that apply

(i) No

(ii) Segregate by data type (sensitive personal, personal and critical)

(iii) Segregate by geography

13. Please rank the following in order of how you think they influence the decision of where a company's data centre should be located

Serial No.	Factor	Rank
(i)	Fixed cost of using/ building a storage facility	
(ii)	Variable cost of using a storage facility	
(iii)	Availability of other supporting infrastructure	
(iv)	Performance and scalability of the facility	
(v)	Availability of human capital	
(vi)	Data Security	
(vii)	Regulatory predictability	
(viii)	Technical efficiency and managing latency	
(ix)	Client preferences	
(x)	Climate and environment	

14a. What is the approximate share of ICT costs in the overall operating costs of your business (please include costs of software, server capacity purchased/ built, personnel, database purchased for all IT related functions of your company)

(i) 0%

(ii) 0% – 5%

(iii) 5% - 10%

(iii) 10% – 30%

(iv) 30% – 50%

(v) > 50%

14a. What is the approximate share of ICT costs in the overall operating costs of your business (please include costs of software, server capacity purchased/ built, personnel, database purchased for all IT related functions of your company)

(i) 0%

(ii) 0% – 5%

(iii) 5% - 10%

(iii) 10% – 30%

(iv) 30% – 50%

(v) > 50%

14b. What is the approximate share of data management costs in the overall ICT costs of your business (please include costs of software, server capacity purchased/ built, personnel purchased only for collection, processing and storage of data.)

(i) 0%

(ii) 0% – 5%

(iii) 5% - 10%

(iii) 10% – 30%

(iv) 30% – 50%

(v) > 50%

14c. What is the share of fixed and variable costs of data management?

(i) Fixed Cost or One-time cost _____

(ii) Variable Cost or Recurring cost _____

14d. If answer to Question 12 is marked as (i) No, (i.e. your company does not segregate data) what will be the additional costs for data segregation to your company?

(i) Additional 0 - 10 % of your total data management costs

(ii) Additional 10% - 30% of your total data management costs

(iii) Additional 30% - 50% of your total data management costs

(iv) Additional 50% - 100% of your total data management costs

(v) Addition of more than 100% to your data management costs

15. Please list all the current data localisation policies that your organization complies with (Localisation measures are policy mandates for storing certain types of data domestically)

(i) _____

(ii) _____

(iii) _____

(iv) _____

(v) _____

C. Impact of Data Management (Localisation) Regulations

Questions 15 and 16 are not applicable if the company doesn't uses servers located outside India or if business processes do not entail cross-border flow of data

15. What will be impact on your ICT costs if the proposed data localisation measures were to be implemented?

Implications on Cost	Regulations that demand:		
	Local storage of data but do not prohibit its cross border transfer	Local storage of data and restrict transfer only to countries with recognized privacy standards	Local storage of data and completely restrict data transfers
Decrease by > 50%			
Decrease by 10% - 50%			
Decrease by <10%			
No Impact			
Increase by <10%			
Increase by 10% - 50%			
Increase by >50%			

16. What will be the impact on your data management costs if the proposed data localisation measures were to be implemented?

Implications on Cost	Regulations that demand:		
	Local storage of data but do not prohibit its cross border transfer	Local storage of data and restrict transfer only to countries with recognized privacy standards	Local storage of data and completely restrict data transfers
Decrease by > 50%			
Decrease by 10% - 50%			
Decrease by <10%			
No Impact			
Increase by <10%			
Increase by 10% - 50%			
Increase by >50%			

17. How will data localisation regulations (storage and transfer) in India impact your business potential? (Select all that apply)
    (i) Lower competitiveness versus other manufacturers/ service providers in the industry
    (ii) Improve competitiveness versus other manufacturers/ service providers in the industry
    (iii) Lower cost to downstream companies/ individuals
    (iv) Increase cost to downstream companies/ individuals
    (v) Lower the quality of service offered/ product manufactured
    (vi) Improve the quality of service offered/ product manufactured
    (vii) None of the above

18a. Do data localisation measures in other countries impact your business in India?
    (i) Yes
    (ii) No

18b. If answer to 18a, is (i) yes, please select top 3 countries whose data localisation policies impact/ likely to impact your business? (Use country code - If there are less than 3, leave some responses blank)
    (i) Country 1 _____
    (ii) Country 2 _____
    (iii) Country 3 _____

18c. If answer to 18a, is (i) yes, how do/will data localisation regulations (storage and transfer) in other countries impact your business potential in India? (Select all that apply)
    (i) Lower competitiveness versus other manufacturers/ service providers in the industry
    (ii) Improve competitiveness versus other manufacturers/ service providers in the industry
    (iii) Lower cost to downstream companies/ individuals
    (iv) Increase cost to downstream companies/ individuals
    (v) Lower the quality of service offered/ product manufactured
    (vi) Improve the quality of service offered/ product manufactured
    (vii) None of the above

19a. How in your opinion can data localisation benefit a source economy? (Select all that apply).

Note1: A source economy is one where data is generated and collected

(i) Nurture domestic companies

(ii) Better control over citizen data

(iii) Improve data privacy

(iv) Limit foreign surveillance

(v) Encourage investment in the domestic economy

(vi) Others _____

(vii) None of the above

19b. How in your opinion can data localisation cost a source economy? (Select all that apply)

(i) Lower efficiency and increase costs for domestic firms

(ii) Lower efficiency and increase costs for foreign firms operating in the source country

(iii) Increase national government surveillance

(iv) Patronise industry/ firms

(v) Others _____

(vi) None of the above

20. What in your opinion are alternates to data localisation measures in an economy? (Select all that apply)

(i) Bilateral agreements that provide safe harbor

(ii) Data Mirroring

(iii) Industry measures such as the APEC Cross Border Privacy Rules System

(iv) Measures to organically improve domestic investment in data servers

(v) Others _____

(vi) None of the above