The Localisation Gambit

Unpacking Policy Measures for Sovereign Control of Data in India

19th March, 2019

By **Arindrajit Basu, Elonnai Hickok, and Aditya Singh Chawla**
Edited by **Pranav M Bidare, Vipul Kharbanda, and Amber Sinha**
Research Assistance **Anjanaa Aravindan**

The Centre for Internet and Society, India

Acknowledgements

The authors would like to thank Pranav MB, Vipul Kharbanda, Amber Sinha, and Saumyaa Naidu for their invaluable edits and comments on the draft. It also greatly benefited from insights derived from conversations with Rahul Matthan, Vinay Kesari, Sunil Abraham, Parminder Jeet Singh,Ambika Khanna, Siddharth Sonkar, and Karan Saini. It was also greatly improved due to a colloquium held at the Trilegal Office in Bangalore. The paper immensely benefited from all these insights but any errors and inaccuracies remain the authors alone.

Executive Summary

The vision of a borderless internet that functions as an open distributed network is slowly ceding ground to a space that is greatly political, and at risk of fragmentation due to cultural, economic, and geo-political differences. A variety of measures for asserting sovereign control over data within national territories is a manifestation of this trend.

Over the past year, the Indian government has drafted and introduced multiple policy instruments which dictate that certain types of data must be stored in servers located physically within the territory of India. These localization gambits have triggered virulent debate among corporations, civil society actors, foreign stakeholders, business guilds, politicians, and governments. This White Paper seeks to serve as a resource for stakeholders attempting to intervene in this debate and arrive at a workable solution where the objectives of data localisation are met through measures that have the least negative impact on India's economic, political, and legal interests.

We begin this paper by studying the pro-localisation policies in India. We have defined data localisation as 'any legal limitation on the ability for data to move globally and remain locally.'[1] These policies can take a variety of forms. This could include a specific requirement to locally store copies of data, local content production requirements, or imposing conditions on cross border data transfers that in effect act as a localization mandate.[2]

Presently, India has four sectoral policies that deal with localization requirements based on type of data, for sectors including banking, telecom, and health - these include the RBI Notification on 'Storage of Payment System Data', the FDI Policy 2017, the Unified Access License, and the Companies Act, 2013 and its Rules, The IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017, and the National M2M Roadmap.

[1] Joshua Meltzer, 'The Internet, Cross-Border Data Flows and International Trade' [2013] Issues in Technology Innovation 16 <https://www.brookings.edu/wp-content/uploads/2016/06/internet-dataand-trade-meltzer.pdf>.

[2] For instance, some countries, such as Malaysia, permit transfers only with the explicit consent of the data subject. In some cases, this can serve as a significant impediment.

At the same time, 2017 and 2018 has seen three separate proposals for comprehensive and sectoral localization requirements based on type of data across sectors including the draft Personal Data Protection Bill 2018, draft e-commerce policy, and the draft e-pharmacy regulations.

The policies discussed reflect objectives such as enabling innovation, improving cyber security and privacy, enhancing national security, and protecting against foreign surveillance. The subsequent section reflects on the objectives of such policy measures, and the challenges and implications for individual rights, markets, and international relations.

We then go on to discuss the impacts of these policies on India's global and regional trade agreements. We look at the General Agreement on Trade in Services (GATS) and its implications for digital trade and point out the significance of localisation as a point of concern in bilateral trade negotiations with the US and the EU.

We then analyse the responses of fifty-two stakeholders on India's data localisation provisions using publicly available statements and submissions. Most civil society groups - both in India and abroad are ostensibly against blanket data localisation, in the form by which it is mandated by the Srikrishna Bill. Foreign stakeholders including companies such as Google and Facebook, politicians including US Senators, and transnational advocacy groups such as the US-India Strategic Partnership Forum, were against localisation citing it as a grave trade restriction and an impediment to a global digital economy which relies on the cross-border flow of data. The stance taken by companies such as Google and Facebook comes as no surprise, since they would likely incur huge costs in setting up data centres in India if the localisation mandate was implemented.

Stakeholders arguing for data localisation included politicians and some academic and civil society voices that view this measure as a remedy for 'data colonialism' by western companies and governments. Large Indian corporations, such as Reliance, that have the capacity to build their own data centres or pay for their consumer data to be stored on data servers support this measure citing the importance of 'information sovereignty.' However, industry associations such as NASSCOM and Internet and Mobile Association of Indian (IAMAI) are against the mandate citing a negative impact on start-ups that may not have the financial capacity to fulfil the compliance costs required. Leading private players in the digital economy, such as Phone Pe and Paytm support the mandate on locally storing payments data as they believe it might improve the condition of financial security services.

As noted earlier, various countries have begun to implement restrictions on the cross-border flow of data. We studied 18 countries that have such mandates and found that models can differ on the basis of the strength and type of mandate, as well as the type of data to which the restriction applies, and sectors to which the mandate extends to. These models can be used by india to think through potential means of pushing through a localisation mandate.

Our research suggests that the various proposed data localization measures, serve the primary objective of ensuring sovereign control over Indian data. Various stakeholders have argued that data localisation is a way of asserting Indian sovereignty over citizens' data and that the data generated by Indian individuals must be owned by Indian corporations.[3] It has been argued that Indian citizens' data must be governed by Indian laws, security standards and protocols.[4]

However, given the complexity of technology, the interconnectedness of global data flows, and the potential economic and political implications of localization requirements - approaches to data sovereignty and localization should be nuanced. In this section we seek to posit the building blocks which can propel research around these crucial issues. We have organized these questions into the broader headings of prerequisites, considerations, and approaches:

PRE-REQUISITES

From our research, we find that any thinking on data localisation requirements must be preceded with the following prerequisites, in order to protect fundamental rights, and promote innovation.

- **Is the national, legal infrastructure and security safeguards adequate to support localization requirements?**
- **Are human rights, including privacy and freedom of expression online and offline, adequately protected and upheld in practice?**
- **Do domestic surveillance regimes have adequate safeguards and checks and balances?**

[3] See Annexure

[4] L Kathragadda and A Sengupta, "A Digital Dandi March:Push data localisation to preserve sovereignty and enable fair competition", 2018, <https://timesofindia.indiatimes.com/blogs/toi-edit-page/a-digital-dandi-march-push-data-localisation-to-preserve-indias-sovereignty-and-enable-fair-competition/>

- **Does the private and public sector adhere to robust privacy and security standards and what should be the measure to ensure protection of data?**

CONSIDERATIONS

- **What are the objectives of localization?**
    a. **Innovation and Local ecosystem**
        i. The Srikrishna Committee Report specifically refers to the value in developing an indigenous Artificial Intelligence ecosystem. Much like the other AI strategies produced by the NITI Aayog and the Task Force set up by the Commerce Department, it states that AI can be a key driver in all areas of economic growth, and cites developments in China and the USA as instances of reference.
    b. **National Security, Law Enforcement and Protection from Foreign Surveillance**
        i. As recognised by the Srikrishna White Paper, a disproportionate amount of data belonging to Indian citizens is stored in the United States, and the presently existing Mutual Legal Assistance Treaties process (MLATs) through which Indian law enforcement authorities gain access to data stored in the US is excessively slow and cumbersome.
        ii. The Srikrishna Committee report also states that undersea cable networks that transmit data from one country to another are vulnerable to attack.
        iii. The report suggests that localisation might help protect Indian citizens against foreign surveillance.

- **What are the potential spill-overs and risks of a localisation mandate?**
    a. **Diplomatic and political:** Localisation could impact India's trade relationships with its partners.
    b. **Security risks ("Regulatory stretching of the attack surface"):** Storing data in multiple physical centres naturally increases the physical exposure to exploitation by individuals physically obtaining data or accessing the data remotely. So, the infrastructure needs to be backed up with robust security safeguards and significant costs to that effect.
    c. **Economic impact:** Restrictions on cross-border data flow may harm overall economic growth by increasing compliance costs and entry barriers for foreign service providers and thereby reducing investment or passing on these costs to the consumers. The major compliance issue

is the significant cost of setting up a data centre in India combined with the unsuitability of weather conditions. Further, for start-ups looking to attain global stature, reciprocal restrictions slapped by other countries may prevent access to the data in several other jurisdictions.

- **What are the existing alternatives to attain the same objectives?**
  The objective and potential alternatives are listed below:

OBJECTIVE	**ALTERNATE**
Law enforcement access to data	Pursuing international consensus through negotiations rooted in international law
Widening tax base by taxing entities that do not have an economic presence in India	Equalisation levy/Taxing entities with a Significant Economic Presence in India (although an enforcement mechanism still needs to be considered).
Threat to fibre-optic cables	Building of strong defense alliances with partners to protect key choke points from adversaries and threats
Boost to US based advertisement revenue driven companies like Facebook and Google ('data colonisation')	Developing robust standards and paradigms of enforcement for competition law

APPROACH

- **What data might be beneficial to store locally for ensuring national interest? What data could be mandated to stay within the borders of the country? What are the various models that can be adopted?**

a. **Mandatory Sectoral Localisation:** Instead of imposing a generalized mandate, it may be more useful to first identify sectors or categories of data that may benefit most from local storage.

b. 'Conditional ('Soft') Localisation: For all data not covered within the localisation mandate, India should look to develop conditional prerequisites for transfer of all kinds of data to any jurisdiction, like the Latin American countries, or the EU. This could be conditional on two key factors:

1. **Equivalent privacy and security safeguards:** Transfers should only be allowed to countries which uphold the same standards. In order to do this, India must first develop and incorporate robust privacy and security protections.
2. **Agreement to share data with law enforcement officials when needed:** India should allow cross-border transfer only to countries that agree to share Indian citizens' data with Indian authorities based on the standards

Introduction

The internet was conceptualized as an open distributed network without borders. Yet, as governments recognize the national interest and value in internet infrastructure and data, it has become a highly political space at risk of fragmentation based on differences in culture, economics, and politics.[5] Measures for control over data within national territories have been one manifestation of this. The introduction of these measures in various jurisdictions has lead to heated debate among civil society actors, private sector voices and lawyers, due to the far reaching economic, social and political impact such measures can have.

Over the past year, the Indian government has drafted and introduced multiple policy instruments which dictate that certain types of data must be stored in servers located physically within the territory of India. This includes, the draft Personal Data Protection Bill, 2018, RBI Notifications, and the (retracted then revised) draft e-commerce policy. India is not alone in pushing for such requirements: other countries such as Canada, EU, Russia and China have also introduced policies which have various mandates for the storage and processing of personal data within the ambit of national laws. This paper examines such legal rules, administrative guidelines, or practices that dictate or influence the localization of data for its storage or processing.[6] We hope that this paper serves as a useful frame of reference for policy-makers and academics attempting to grapple with some of the critical questions in the data localisation debate.

First, we examine definitions and conceptualizations of policy measures for exerting control over data within national territories. We then embark upon a mapping of the recent measures towards national control of data in India with respect to proposed and enacted policy. Following that, we reflect on the various objectives of localisation and deconstruct the various alternate routes to attaining the same objectives. We then go onto understand the implications of these measures for India's trade commitments. Finally, we present a sample of the different approaches to data localization that have been adopted in other jurisdictions, with the aim of

[5] Jim Foster, Managing The Global Internet Economy: A New Challenge For The Us And Japan, 2015, <https://www.brookings.edu/wp-content/uploads/2015/03/james-foster-presentation.pdf>
[6] Staff Working Document on the free flow of data and emerging issues of the European data economy, European Commission, 10 January 2017 <https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy>

understanding different models and mechanisms for legally enabling such requirements. In the concluding section, we summarise learnings from the article and attempt to articulate a set of questions that can be useful when developing a framework that would result in greater national control of data. It also explores if a range of policy tools can potentially come together to achieve similar objectives.

Methodology

When drafting this paper, empirical, technical or economic analysis was not conducted to confirm or map the consequences of the policy measures we studied. Instead, we relied on a comparative assessment of similar measures introduced across the world to study the legal and political motives and efficacy of these instruments. When we endeavour to understand the pros and cons of data localisation, it is crucial to consider that many of the potential impacts discussed here are based on projections driven by modeling conducted in other jurisdictions.This data may suffer from its own flaws, and the insights may not necessarily translate to the Indian context. Therefore, throughout the paper, we attempt to distinguish projected harms or benefits from more concrete legal arguments that we make in the context of restricting cross-border data transfers.

We would also like to point out that while equal efforts and resources have been dedicated for researching both the pros and cons of data localisation, the paper has been able to map a higher number of arguments against data localisation as compared to arguments in favour of localisation. Although this might make the paper appear to be biased against data localisation, it has never been the intention of the authors and all efforts have been made to ensure that the paper is as neutral as possible. Our recommendations take this into account. We attempt to strike a middle ground by advocating for a restricted and conditional localisation mandate, as an alternative to the broad mandate introduced in the Srikrishna Bill.

Defining and Conceptualizing Sovereign Control of Data

Before we begin, it is useful to identify the definitions of a variety of terms that have been used by several stakeholders both in India and abroad in the context of sovereign control of data. Data localization, data residency, data nationalism, and

data sovereignty are terms that have broadly been used to describe requirements to ensure a nation's control over data generated within its borders. Though these terms are often used interchangeably, for the purpose of this paper, we hope to explore the nuances and similarities of each term.

Data Localization and Data Residency

Requirements for local storage and processing of data are commonly referred to as **'data localization'** or **'data residency'** requirements. Data localisation can broadly be defined as 'any legal limitation on data moving globally and compelling it to remain locally.[7] These policies can take a variety of forms. This could include a specific requirement to locally store copies of data, local content production requirements, or imposing conditions on cross border data transfers that in effect act as a localization mandate.[8]

Data Nationalism, Data Protectionism, Data Sovereignty and Data Colonialism

Policies that seek to ensure domestic control over data have been termed as 'data nationalism'.[9] **'Data exceptionalism'** is a school of thought that argues that data is un-territorial and therefore incompatible with existing concepts of territorial jurisdiction. [10]However, there are a number of scholars who have opposed 'data exceptionalism' and argue that territorial jurisdiction can be asserted over data.[11] The assertion of territoriality is the building blocks for any argument justifying data localisation.

'Data nationalism' is a framing device that refers to the broader trend of countries asserting the primacy of national priorities (related to law enforcement, privacy,

---

[7] Joshua Meltzer, 'The Internet, Cross-Border Data Flows and International Trade' [2013] Issues in Technology Innovation 16
<https://www.brookings.edu/wp-content/uploads/2016/06/internet-dataand-trade-meltzer.pdf>.

[8] For instance, some countries, such as Malaysia, permit transfers only with the explicit consent of the data subject. In some cases, this can serve as a significant impediment.

[9] See for instance : Anupam Chander, Uyên P. Lê, Data Nationalism, 64 Emory L.J. 677 (2015), <http://law.emory.edu/elj/content/volume-64/issue-3/articles/data-nationalism.html>;
D. Castro, The False Promise of Data Nationalism, December 2013,
<http://www2.itif.org/2013-false-promise-data-nationalism.pdf>;
C. Kuner, Data Nationalism And Its Discontents, Emory Law Journal, 2015
<https://brusselsprivacyhub.eu/onewebmedia/kuner.pdf>.

[10] See,for example Zachary D. Clopton, Territoriality, Technology, and National Security, 83 U. CHI.L.REV. 45 (2016

[11] A.Woods, Against Data Exceptionalism,Stanford Law Review, 2016
https://uknowledge.uky.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1593&context=law_facpub

security, etc) over the vision of a global internet.[12] **'Data protectionism'** is a manifestation of data nationalism may indicate imposing restrictions on cross-border transfers of data as a matter of economic policy.[13] Mandating local storage of data can be an element of such an agenda.

'Data sovereignty' is a connected phrase-which basically is a guarantee towards ensuring that national law applies to data even if it is outside of a nation's territory.[14] Other scholars have alternate understandings of data sovereignty, which necessarily entail keeping data within national territories.[15]

'Data colonialism' is another term that has been used widely in India and other countries to justify data localisation. Broadly, an understanding of **'Data colonialism'** refers the extractive practices of modern day western digital companies through data-driven revenue generation and behavioural modification, which are analogous to predatory colonial practices of the past.[16]

Therefore, the manner in which a localisation gambit is enforced will determine how it fits into the apparatus of data nationalism. The goal should be to further 'data sovereignty' without engaging in excessive 'protectionism' such that India can assert it's laws without falling foul of diplomatic or legal agreements with foreign stakeholders.

Mapping of Current Policy Measures for Localization of Data in India

This section examines various current and proposed instruments that mandate data localization in India. Presently, India has in place four sectoral policies that include localization requirements based on type of data including in the banking, telecom, and health sectors - these include the RBI Notification on 'Storage of Payment

[12] C. Kuner, Data Nationalism And Its Discontents, Emory Law Journal, 2015 <https://brusselsprivacyhub.eu/onewebmedia/kuner.pdf>
[13] M.F. Ferracane, E. Marel, The Cost of Data Protectionism, October 2018, <http://ecipe.org/blog/the-cost-of-data-protectionism/>
[14] C. Chelliah, With Data Sovereignty, Location Isn't Everything, <https://www.oracle.com/uk/cloud/paas/features/data-sovereignty/>
[15] J Labour, Data sovereignty: What you need to know and why you should care, 24 January 2018 <https://cira.ca/blog/state-internet/data-sovereignty-what-you-need-know-and-why-you-should-care>
[16] Couldry, Nick and Mejias, Ulises (2018) Data colonialism: rethinking big data's relation to the contemporary subject. Television and New Media. ISSN 1527-4764

System Data', the FDI Policy 2017, the Unified Access License, and the Companies Act, 2013 and its Rules.

At the same time, 2017 and 2018 has seen three separate proposals for comprehensive and sectoral localization requirements based on type of data across sectors including the draft Personal Data Protection Bill 2018, draft e-commerce policy, and the draft e-pharmacy regulations. Localisation requirements have been included in these instruments due to a number of reasons including national security, economic growth, innovation, and protection against foreign surveillance. Below we examine the different proposed and existing requirements in detail.

The Draft Personal Data Protection Bill, 2018

In August 2017, the Ministry of Electronics and Information Technology had constituted a committee of experts, Chaired by the Retired former judge of the Supreme Court, Justice B N Srikrishna. The Committee was tasked with examining issues related to data protection in India, and formulating a draft data protection statute.[17] In July 2018, the Committee released its Report, as well as the proposed Draft Personal Data Protection Bill, 2018. The Draft was open for comments from the public till October 10, 2018.[18] The final draft will eventually be presented to the Ministry for consultation, which may make further amendments before introducing it in Parliament. The Bill brings together requirements for data localization and data sovereignty by extending the applicability of the Act to data fiduciaries outside of India under certain circumstances and through explicit localization requirements.

Section 2 subsection 2 of the draft extends the applicability of the law to the processing of personal data by data fiduciaries or data processors not present within the territory of India, only *if such processing is — (a) in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within the territory of India; or (b) in connection with any activity which involves profiling of data principals within the territory of India.*

[17] Office Memorandum: Constitution of a Committee of Experts to deliberate on a data protection framework for India, Ministry of Electronics & Information Technology, Government of India, 31 July 2017
<https://meity.gov.in/writereaddata/files/meity_om_constitution_of_expert_committee_31072017.pdf>

[18] White Paper on Data Protection framework for India - Public Comments invited, Ministry of Electronics & Information Technology, Government of India,
<https://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited>

Section 40 of the draft mandates that data fiduciaries[19] must maintain a serving copy of all personal data within the territory of India: This section adopts a three-pronged model charting out the transfer of data outside India.

- First, as per Section 40(1), all personal data to which the Bill applies must have at least one live, serving copy stored inside India.

- Second, certain categories of personal data may be notified as 'critical personal data' by the central government under Section 40(2). This data may be stored and processed only in India, such that no transfer abroad is permitted.

- Third, under Section 40(3), the Central government has been bestowed with the power to exempt transfers on the basis of strategic or practical concerns, thereby enabling the free flow of data when they deem it to be justified. However, these exemptions cannot be made for 'sensitive personal data' under the Bill.[20]

Section 41 further imposes conditions on the transfer of personal data outside of India. Personal data may only be transferred abroad under the following circumstances:

Standard contractual clauses or intra-group schemes

Personal data may be transferred pursuant to standard contractual clauses or intra-group schemes previously approved by the Data Protection Authority.[21] Such approval is conditional on the mechanisms being able to effectively protect the rights of data principals.[22] Further, data fiduciaries must periodically certify compliance with the clauses or schemes, and must bear all liability for harms caused

[19] Section 3(13). "Data fiduciary" means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data.

[20] "Section 40 'Restrictions on Cross-Border Transfer of Personal Data':

Every data fiduciary shall ensure the storage, on a server or data centre located in India, of at least one serving copy of personal data to which this Act applies.

(1) The Central Government shall notify categories of personal data as critical personal data that shall only be processed in a server or data centre located in India.

(2) Notwithstanding anything contained in sub-section (1), the Central Government may notify certain categories of personal data as exempt from the requirement under sub-section (1) on the grounds of necessity or strategic interests of the State.

(3) Nothing contained in sub-section (3) shall apply to sensitive personal data."

[21] Section 41(1)(a).

[22] Section 41(5).

by any non compliance.[23] Data may also be transferred pursuant to consent from the data principal.[24] For transfers of sensitive personal data, such consent must be explicit.[25] However, this excludes critical personal data, as notified under Section 40.

Countries or international organizations that provide an adequate level of protection
Transfers may also be made to countries (or specific sectors in a country), or international organizations that have been previously approved by the Central Government.[26] Such entities must provide an adequate level of protection to personal data. This may be determined by any applicable laws or international agreements, and the possibility of effective enforcement. The Government must periodically review its findings to ensure that data remains adequately protected.[27]

Necessity
A particular transfer or set of transfers may be approved by the Authority on the grounds of necessity.[28] Sensitive personal data may also be transferred to fiduciaries engaged in the provision of health or emergency services, if the processing is for purposes related to employment.[29] Such transfers must be notified to the authority within a prescribed time period.[30] Transfers to specific countries or international organizations may also be allowed if the Central Government is satisfied that the transfer would not hamper the effective enforcement of the Act.[31] Notably, such transfers are also permitted for critical personal data (which must ordinarily be stored exclusively within India).

In terms of enforcement, the Bill does not prescribe any specific penalty for violating Sections 40 and 41. Thus, the general penalty under Section 73 of the Bill would be applicable in cases where fiduciaries fail to comply with the provisions.[32] In addition,

[23] Section 41(6).
[24] Section 41(1)(d).
[25] Section 41(1)e).
[26] Section 41(1)(b).
[27] Section 41(2).
[28] Section 41(1)(c).
[29] Section 41(3)(a); Section 16.
[30] Section 41(4).
[31] Section 41(3)(b).
[32] Section 73. Penalty for contravention where no separate penalty has been provided.—Where any person fails to comply with any provision of this Act, or rules prescribed or regulations specified thereunder as applicable to such person, for which no separate penalty has been provided, then such person shall be liable to a penalty subject to a maximum of one crore rupees in case of significant data fiduciaries, and a maximum of twenty five lakh rupees in all other cases.

Section 90 prescribes criminal punishment,[33] when personal data is transferred in contravention of the Act which results in 'significant harm'[34] to data principals. Similarly, Section 91 prescribes punishment,[35] when 'sensitive personal data'[36] is transferred causing 'harm'[37] to data principals.

However, ***the Bill is currently in draft stage, and it is unclear when it will be enacted into law.*** Further, Section 97(7) enables the Central Government to notify Section 40 at a date later than the passage of the Bill.[38] ***This implies the possibility that the mandate for data localization under India's data protection law might not come into force with the enactment of the statute.***

[33] Section 90. Obtaining, transferring or selling of personal data contrary to the Act.—Any person who alone or jointly with others, knowingly or intentionally or recklessly, in contravention of the provisions of this Act—(a) obtains personal data; or (b) discloses personal data; or © transfers personal data to another person; or(d)sells or offers to sell personal data to another person,which results in significant harm to a data principal, then such person shall be punishable with imprisonment for a term not exceeding three years or shall be liable to a fine which may extend up to rupees two lakh or both.
[34] Section 3(37). "Significant harm" means harm that has an aggravated effect having regard to the nature of the personal data being processed, the impact, continuity, persistence or irreversibility of the harm;
[35] Section 91. Obtaining, transferring or selling of sensitive personal data contrary to the Act.—Any person who alone or jointly with others, knowingly or intentionally or recklessly, in contravention of the provisions of this Act—(a) obtains sensitive personal data; or (b) discloses sensitive personal data; or(c)transfers sensitive personal data to another person; or (d) sells or offers to sell sensitive personal data to another person, which results in harm to a data principal, then such person shall be punishable with imprisonment for a term not exceeding five years or shall be liable to a fine which may extend up to rupees three lakhs or both.

[36] Section 3(35). "Sensitive Personal Data" means personal data revealing, related to, or constituting, as may be applicable—(i) passwords; (ii) financial data; (iii) health data; (iv) official identifier; (v) sex life; (vi) sexual orientation; (vii) biometric data; (viii) genetic data;(ix) transgender status; (x) intersex status; (xi) caste or tribe; (xii) religious or political belief or affiliation; or (xiii) any other category of data specified by the Authority under section 22.
[37] Section 3(21). "Harm" includes—(i) bodily or mental injury; (ii) loss, distortion or theft of identity; (iii) financial loss or loss of property, (iv) loss of reputation, or humiliation; (v) loss of employment; (vi) any discriminatory treatment;4(vii)any subjection to blackmail or extortion;(viii)any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal; (ix) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; or (x) any observation or surveillance that is not reasonably expected by the data principal.
[38] "97. Transitional provisions and commencement.—
[...]
(7) Section 40 shall come into force on such date as is notified by the Central Government for the purpose of that section."

Draft E-commerce Policy (s)[39]

The Department of Industrial Policy and Promotion (DIPP) has circulated two seperate drafts of a draft e-commerce policies. The first of these policies was circulated in July 2018 and was subsequently retracted after strong opposition from key stakeholders.[40] A revised policy was circulated in February and was opened to stakeholder comments, which are due by March 29th,2019.[41]

Version 1

In July 2018, the Government circulated a draft E-Commerce Policy among stakeholders.[42] One of the proposals in the Policy, was the requirement of local storage of data.

According to Clause 2.3, *"the following categories of data would be required to be stored exclusively in India and suitable framework developed for sharing the data within the country (this would be guided by ongoing exercises, including the forthcoming Report of the Justice Srikrishna Committee):*

- *Community data collected by IoT devices in public space; and*
- *Data generated by users in India from various sources including e-commerce platforms, social media, search engines etc"*[43]

Further, Clause 2.4 states that:
"The development of cutting-edge and innovative technologies in India would be promoted by ensuring access to data through the following:

- *The Government would have access to data stored in India for national security and public policy objectives subject to rules related to privacy, consent etc.*
- *Data stored in India should be shared with start-ups meeting the stipulated criteria (turnover of Rs.50 crore etc.)*

[39] The DIPP has amended the provisions wrt ecommerce in the FDI circular. As of the date of publication of this paper, there is no clarity on whether it is a new iteration of the originally released policy, or if it's a separate exercise. The latter is more likely because the scope seems to be limited to FDI, while the original policy was broader
[40]https://www.livemint.com/Politics/6XHK8WiNeAtphz8GPIwY5H/Govt-rethinks-ecommerce-policy-on-stakeholder-objections.html
[41]" DPIIT extends deadline for comments"https://www.livemint.com/politics/policy/dpiit-extends-deadline-for-public-comments-on-draft-e-commerce-policy-1552394797242.html
[42] Electronic Commerce in India: Draft National Policy Framework, <https://www.medianama.com/wp-content/uploads/Draft-National-E-commerce-Policy.pdf>
[43] Ibid Clause 2.3

- *At the request of the consumer, data generated by her in India through various channels, including e-commerce platforms, social media, search engines etc., would be allowed to be portable amongst platforms in India."*[44]

Thus, though the policy reflects similar sentiments to the draft Data Protection Bill in the potential for local storage of data to strengthen national security, the policy places more emphasis on the proposition that storage of data exclusively in India may serve the purpose of national security, as well as enabling innovation by ensuring access to data for the startup ecosystem that the Draft Bill.

Version 2

The draft e-commerce policy has now been retracted. However, in February 2019, another draft was circulated that retained the localisation requirements through the following provisions:

1.1 A legal and technological framework to be created that can provide the basis for imposing restrictions on cross-border data flow from the following specified sources
a) Data collected by IoT devices installed in public space; and
b) Data generated by users in India by various sources, including ecommerce platforms, social media, search engines etc.
The legal and technological framework would also provide basis for sharing the data collected by IoT devices under (a) above with domestic entities for use in research and development for public policy purposes.

The revised policy goes onto explain[45] that any business entity that processes sensitive data in India and stores the same abroad must : (1) Not make it available to other business entities or third parties even if the customer consents to it, (2) Not make data stored abroad available to foreign governments without the permission of the Indian government, (3) Any request from the Indian authorities to have accessed to such data stored abroad must be complied with immediately.

The revised policy also contains a set of exceptions[46] to which it recommends restrictions on cross-border data flows should not apply to. These include (a) Data that is not collected in India, (b) B2B data which is sent to India as a part of a commercial contract between a foreign and Indian business entity, (c) Software and cloud computing services involving technology related data flow which have no personal or community implications, (d) MNCs moving data internal to the company.

[44] Ibid Clause 2.4
[45] Draft Clause 1.2
[46] Draft Clause 1.3

Point (c) is fairly vague and does not clearly explain how 'technology related data' is distinguishable from that with 'community or personal' implications.

RBI Notification on 'Storage of Payment System Data'

On 6th April 2018, the Reserve Bank of India issued a circular mandating that all data related to payment systems should be locally stored in India.[47] The Circular states that :

1. *"All system providers shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction. For the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required."*

The primary objective of this policy appears to be to facilitate supervision and monitoring of payment systems in India by the RBI in order to detect suspicious or fraudulent activity.

The directive has been issued under Section 10(2) read with Section 18 of Payment and Settlement Systems Act, 2007. This implies that non compliance could result in imprisonment and penalties pursuant to Sections 26 and 27 of the Act. More importantly it could lead to cancellation of the license to operate as a Payment System or higher fiscal penalties as provided under the license itself.

The Circular allowed six months for compliance, with a compliance report to be submitted to the RBI by October 15, 2018. In addition, it mandated that a system audit should be conducted by CERT-IN empaneled auditors in order to certify compliance, with the report to be submitted by December 31, 2018.[48] It is unclear from publicly available information the extent to which these conditions have been fulfilled by banks operating in India.

[47] RBI Notification: Storage of Payment System Data, 6 April 2018, <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0>
[48] Ibid.

Draft E-Pharmacy Regulations

In August 2018, the Central Government released a draft set of rules to regulate online pharmacies in India. This was in the form of amendments to the Drugs and Cosmetics Rules, 1945.[49]

The proposed Rule 67K (3) mandates that :
"The e-pharmacy portal shall be established in India through which they are conducting the business of e-pharmacy and shall keep the data generated localised:

Provided, that in no case the data generated or mirrored through e-pharmacy portal shall be sent or stored, by any means, outside the India."

The draft rules were notified on August 28, 2018 with a period of 45 days to receive comments and objections. However, as of the time of writing, a final version of the rules has not been released or notified.

FDI Policy 2017

The Consolidated FDI Policy Circular of 2017 mandates certain conditions for the Broadcasting Sector.[50] Clause 1.3(ix) states states that : *"the Company shall not transfer the subscribers' databases to any person/place outside India unless permitted by relevant law."*

Fines for non compliance with any stipulation have been prescribed in Clause 3.1, Annexure 6 of the Policy.

National Telecom M2M Roadmap

The National Telecom M2M Roadmap was one of the first policies that hinted towards a data localisation gambit. Released in 2015, the Roadmap stated that : "*From security perspective, there is a strong case for all M2M Gateways and application servers, servicing the customers in India, to be physically located in India."* At the same time,

[49] Ministry Of Health And Family Welfare (Department of Health and Family Welfare), Notification: Amendment to the Drugs and Cosmetics Rules (1945), 28 August 2018 <http://www.cdsco.nic.in/writereaddata/2018_08_28_Draft%20GSR%20817(E)_Sale%20of%20Drugs%20by%20E-Pharmacy.pdf>
[50] Department of Industrial Policy and Promotion, Ministry of Commerce and Industry, Government of India, Consolidated FDI Policy, 2017, <http://dipp.nic.in/sites/default/files/CFPC_2017_FINAL_RELEASED_28.8.17.pdf#107>

the Roadmap noted several concerns, such as the inability of smaller players to comply with such requirements. Further, it noted that India's position should be informed by practices adopted by other countries, on account of "trade reciprocity, privacy, non disclosure conditions etc."[51]

Unified Access License for Telecom

Telecommunication and Internet Service Providers in India must comply with the provisions of the Unified Access License. Clause 39.23(viii) of the License states that :

"The Licensee shall not transfer the following to any person/place outside India:-

a. *Any accounting information relating to subscriber (except for international roaming/billing) (Note: it does not restrict a statutorily required disclosure of financial nature) ; and*
b. *User information (except pertaining to foreign subscribers using Indian Operator's network while roaming and IPLC subscribers)."*

The stipulation falls under Chapter IV of the License, titled 'Security Conditions'. Thus, the mandate for local storage of data is based on security related concerns.

Clause 10 of the License empowers the Department of Telecommunications to impose penalties, or suspend or revoke the license for non compliance.

Companies Act, 2013 and Rules

Entities to which the Companies Act, 2013 applies are required to maintain books of accounts for audit and inspection in compliance with the Act and related regulations. In particular, Rule 3(5) of the Companies (Accounts) Rules, 2014 mandates that "the back-up of the books of account and other books and papers of the company maintained in electronic mode, including at a place outside India, if any, shall be kept in servers physically located in India on a periodic basis."

Thus, the Rules require that a copy of the electronic books of accounts should be maintained on servers in India.

[51] Department of Telecommunications, Ministry of Electronics and Information Technology, Government of India, National Telecom M2M Roadmap, 2015, <http://dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf> pp.23

The above conditions, read with Section 128 of the Companies Act, 2013, entail that a violation of the requirements may result in imprisonment or penalty.

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

The Insurance Regulatory and Development Authority enacted the IRDAI (Outsourcing of Activities by Indian Insurers) Regulations in 2017.[52] The Regulations apply to all insurers registered with the IRDAI, with respect to any outsourcing arrangements they may enter into. Rule 18 of the Regulations ("Regulatory Access") mandates that all original policyholder records continue to be maintained in India.

Guidelines on Contractual Terms Related to Cloud Services

In 2017, the Ministry of Electronics and Information Technology released its Guidelines for Government Departments on Contractual Terms Related to Cloud Services under the Meghraj Cloud Initiative.[53] The objective was to highlight key considerations for government departments while procuring cloud services. In particular, the Guidelines focus on key contractual terms that may be incorporated by departments when formulating contracts with cloud providers. The Guidelines propose that "data (text, audio, video, or image files, and software (including machine images), that are provided to the CSP for processing, storage or hosting by the CSP services in connection with the Department's account and any computational results that a Department or any end user derives from the foregoing through their use of the CSP's services)" should be stored within India.[54]

[52] https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx?page=PageNo3149&flag=1
[53]Guidelines for Government Departments On Contractual Terms Related to Cloud Services <http://meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf>
[54] Clause 2.1(d)

TABLE 1: INDIAN LAWS AND POLICIES ENABLING DATA LOCALISATION

Category of Data	**Policy/Law**	**No restriction of cross border flow**	**Cross border flow permitted as long as copy maintained in India**	**No cross border flow permitted**
Critical data	Personal Data Protection Bill, 2018			X
Personal data			X	
Personal data not collected in India		X		
Public IoT data	e-Commerce Policy		X	
E-Commerce data			X	
Payment Systems data	RBI Circular			X
e-Pharmacy data*	e-Pharmacy Regulations			X
Subscriber and User data	Unified Access License for Telecom			X
Subscribers' databases (Broadcasting sector)	FDI Policy			X
Companies' accounts related data	Companies (Accounts) Rules, 2014		X	
Insurance Policyholder data	IRDAI Regulations		X	
Government data	Guidelines on Contractual Terms Related to Cloud		X	

	Services			

Reflecting on Objectives, Challenges and Implications of National Control of Data

The policy measures outlined in the above section reflect objectives such as enabling innovation, improving cyber security and privacy, enhancing national security, and protecting against foreign surveillance. This section reflects on the objectives of such policy measures, and the challenges and implications for individual rights, markets, and international relations.

Enabling Innovation and Economic Growth

With a population of 1.3 billion people, India is a significant market for both foreign and local companies. India is presently home to the 3rd largest corpus of start-ups in the world where Micro, Small and Medium Sized Enterprises (MSMEs) account for 6.11% of India's Gross Domestic Product and 24.63% of GDP from services sector.[55] The Information Technology (IT) sector as a whole makes up about 7.9%.[56] Therefore, considering the impact on MSMEs in the IT sector is critical for policy-makers.

When providing the rationale behind the inclusion of the data localization requirements in the Bill, the Srikrishna Committee Report specifically refers to the value in developing an indigenous Artificial Intelligence ecosystem. Much like the other AI strategies produced by the NITI Aayog and the Task Force set up by the Commerce Department, it states that AI can be a key driver in all areas of economic growth, and cites such eco-systems and developments in China and the USA as instances of reference. The Report also cites a paper authored by Azmeh and Foster which highlights benefits of a data localization policy for developing countries.[57] These benefits include (1) increased foreign direct investment in digital infrastructure

[55] Charting Change Enabling Development, Confederation of Indian Industry, <https://www.cii.in/Sectors.aspx?enc=prvePUj2bdMtgTmvPwvisYH+5EnGjyGXO9hLECvTuNuXK6QP3tp4gPGuPr/xpT2f>

[56] MeITY. (2018). Software and services sector. Ministry of Electronics & Information Technology. <http://meity.gov.in/ content/ software - and - services-sector>

[57] Azmeh, S. and Foster, C.G. (2016) The TPP and the digital trade agenda: Digital industrial policy and Silicon Valley's influence on new trade agreements. Working Paper. International Development, Working Paper Series (16-175). Department of International Development http://eprints.whiterose.ac.uk/125522/

and (2) positive spill-over effects of an indigenous market for data centres through enhanced connection, job creation and the presence of skilled professionals.

Similarly, as envisioned by both versions of the draft e-commerce policy, data that is stored in India could be anonymized and shared with start-ups towards enabling innovation and can be made available to enterprise users if so desired.[58] This vision is complemented by India's national cloud - Meghraj[59] and NITI Aayog's national strategy for Artificial Intelligence and its envisioned National AI Marketplace.[60] Other frameworks for facilitating the sharing of data proposed in the draft e-commerce policy are[61]:

(a) Sharing of data stored in India with start-ups that meet some criteria, which is to be specified (an indication given in the policy is a turn-over of Rs. 50 crore)
(b) At the request of the consumer ('data principal'), social media data to be shared among platforms.

When considering the positive impact that localization may have on start-ups and the locally grown data economy, it is necessary to also take into consideration the projected costs and resulting uncertainties in terms of:

1. Compliance

Local storage of data will mean that companies may need to set up local data centers or pay for data storage services which guarantee that the data shall be stored exclusively in India. Many of these MSMEs use cloud computing services to store the data they are processing, and may not make enough profit at nascent stages in their growth trajectory to offset the fixed costs of setting up cloud centres.[62] A study by Leviathan found that localisation laws could potentially increase costs of setting up

[58] Clause 2.4 ("access to data has emerged as one of the main determinants of success of an enterprise in the digital economy. As India is likely to become one of the largest sources of such commercially useful data in the world, it is imperative that the policy understands and protects the inherent ownership rights to data, and leverages it to ensure that domestic new players are also able to leverage this strength for economic gains by creating innovative digital product")
[59] MeghRaj Cloud Initiative <https://cloud.gov.in/about.php>
[60] Discussion Paper on National Strategy for Artificial Intelligence, NITI Aayog, National Institution for Transforming India, <http://niti.gov.in/content/national-strategy-aidiscussion-paper>
[61] Clause 2.4
[62] N. Shiffman and J. Ben-Avie, Data localization: bad for users, business, and security, June 22, 2018, <https://blog.mozilla.org/netpolicy/2018/06/22/data-localization-india/> ; A. Thaker, India's data localisation plans could hurt its own startups the most, October 16 2018 <https://qz.com/india/1422014/rbis-data-localisation-could-hurt-indias-own-startups/>

servers in a country by 30-60%.[63] Alternatively, setting up data centres is expensive[64] and resource-intensive[65], causing further stress on an already depleted energy sector [66] and is therefore potentially harmful for the environment.[67] According to a 2014 study by the European Centre for International Political Economy (ECIPE), an economy-wide data localisation measure would have caused a GDP loss of 0.8% for India at that point in time.[68] The same report argued that such a policy would reduce the monthly salary of an average worker by 11%.[69] Another 2016 study by the Centre for International Governance Innovation states that even a slightly less stringent localisation regime than the one contemplated by the various instruments discussed might result in India's GDP taking a hit of .25 percentage points.[70]

In addition, data centers are usually highly automated, and allow a small number of works to operate a large facility.[71] Thus, a rise in data centres may not translate into a

[63] ("Brazil has two cloud providers: Amazon and Microsoft. At the low end, for 1GB-equivalent servers, Microsoft's price is US$0.024/hour; the lowest worldwide price for 1GB-equivalent servers, $0.015/hour, would save a Brazilian customer 37.5% on their server costs over a Brazil exclusive solution. For a 2GB-equivalent server, a Brazil-located solution would cost $0.08/hour, and the worldwide cheaper price would be $0.03/hour—a 62.5% savings. Averaged across the types of servers, a customer located in Brazil would pay 54.65% less by using cloud servers outside Brazil, rather than requiring only Brazil-located cloud computing resources.); Leviathan Security Group, Quantifying the Cost of Forced Localization, <https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf>

[64] Google is setting up a data center at The Dalles in Oregon. Total investment into that site i $1.2 billion. The data center in Pryor Creek, Oklahoma went online 2011 at the price of $600,000 and requires another $2 billion investment to continue being used. Another data centre under construction in the Netherlands is expected to cost $773 million. Setting up data centres in india would require further resources spent in cooling the facilities as the locations mentioned are significantly colder than India. Google Data Center FAQ, Part 2 <https://www.datacenterknowledge.com/google-data-center-faq-part-2>

[65] U. Kelkar, Big data is way hotter than you think, 3 Jan 2019 <https://www.livemint.com/Opinion/3kUmycbicdhK81i4GDUuQL/Opinion--Big-data-is-way-hotter-than-you-think.html>

[66] CII, Energy Efficiency in Indian Data Centers: Present Trends and Future Opportunities, June 2013, <https://datacenters.lbl.gov/sites/all/files/CII%20Energy%20Efficieny%20in%20Indian%20Data%20Centers-%20Present%20Trends%20and%20Future%20Opportunities.pdf>

[67] I Burrington (2018),"The environmental toll of a Netflix binge"https://www.theatlantic.com/technology/archive/2015/12/there-are-no-clean-clouds/420744/

[68] Bauer, M., Lee-Makiyama, H., der Marel, E. V. & Verschelde, B., The costs of data localisation: Friendly fire on economic recovery. European Centre for International Political Economy, (2014). <http://www.ecipe.org/app/ uploads/2014/12/OCC320141.pdf>

[69] Ibid.

[70] Bauer, M., Ferracane, M. F. & van der Marel, E. (2016). Tracing the economic impact of regulations on the free flow of data and data localization. Centre for International Governance Innovation and Chatham House, <https://www.cigionline.org/sites/default/files/gcig no30web 2.pdf>

[71] R. Miller, The Economics of Data Center Staffing, January 18 2008, <https://www.datacenterknowledge.com/archives/2008/01/18/the-economics-of-data-center-staffing>

commensurate increase in employment. Reports suggest that data centres may only employ an average of five to thirty people.[72] Further, many of these tend to be highly skilled jobs that may not be recruited locally.[73] Jobs, such as construction work, which tend to come from local sources are one-time costs that would involve the hiring of contract labour,which would cease once the physical construction of the data centre is complete.[74]

As a note, the econometric analysis all the widely quoted studies considered in this section use three basic assumptions to project the impacts of localisation rather than looking at actual impacts of localisation. These assumptions are as follows: (1) Increase in cost price for domestic firms (2) This increase has a downstream linkage and (3) Increased restrictions inhibit firms from sourcing input efficiently, which results in higher costs for firms.

This, in turn, increase prices, which translates to a lower overall Total Factor Production (TFP). The three assumptions are, of course, textbook micro-economic assumptions. However, it is important to remember that the statistics at hand are not empirical realities but projections founded on the assumptions made. An ex post facto assessment of the impacts of localisation on a nation's economy to confirm the projections is important for policy-makers around the globe to truly rely on the numbers.

It is crucial to note that our analysis in this section does not rely on independent modelling conducted by us but on two in-depth studies that have attempted this modelling. However, like Parsheera and Bailey, we make three logical assertions based on our understanding of India's economic set-up at this time. First, it is to be

---

[72] D. Ohara, Synovus Financial Joins Columbia Data Center Neighbors with fewer than 25 employees. Why does Google's data center need 200 employees?, January 12, 2008 <https://www.greenm3.com/gdcblog/2008/1/12/synovus-financial-joins-columbia-data-center-neighbors-with.html>;
A. DeNisco Rayome, Why data centers fail to bring new jobs to small towns, September 19 2016, <https://www.techrepublic.com/article/why-data-centers-fail-to-bring-new-jobs-to-small-towns/>;
J. Lenio, The Mystery Impact of Data Centers on Local Economies Revealed, 2015 <http://www.areadevelopment.com/data-centers/Data-Centers-Q1-2015/impact-of-data-center-development-locally-2262766.shtml>

[73] Q. Hardy, Cloud Computing Brings Sprawling Centers, but Few Jobs, to Small Towns, August 26 2016, <https://www.nytimes.com/2016/08/27/technology/cloud-computing-brings-sprawling-centers-but-few-jobs-to-small-towns.html>

[74]N.Cory.(2017).Cross border data flows:Where are the barriers and what do they cost? InformationTechnologyandInnovation Foundation.Retrieved fromhttps://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost

expected that larger players such as Reliance or PhonePe will be able to afford the costs of localisation more than smaller players, which could explain their staunchly pro-localisation stance.[75] Their competition stems from foreign players seeking to enter the market, and localisation has the potential benefit of eliminating these players while also imposing additional compliance costs on smaller domestic players, at least in the short run.[76] Second, localisation will likely make India an unfeasible market for services that cannot offset the financial or logistical costs of localization.[77] This means that consumers may bear the brunt of this exit by losing access to services that otherwise might be offered. In addition, localisation may lead to country-specific reciprocal measures that may prevent Indian start-ups from expanding globally.[78] Finally, it is crucial to note that merely having more data does not fuel an innovation economy. The relevance of the dataset and the ability to accurately label and process them is crucial for curating a training dataset for an algorithm. Before devising policy measures that improve access to increased quantities of data, debunking India's capacity to process them is an imperative.

2. Technical

Today, data typically flows almost continuously across borders. This is not a functional requirement but the modus operandi for multi-national organisations to optimize costs, security and efficiency. Reisman[79] argues that well developed web services might store data across borders for a number of economic and technical reasons which improve efficiency and lower costs such as Edge Caches,[80] Load

[75] R. Bailey and S. Parsheera (2018)," Data Localisation in India: Questioning the means and ends"https://macrofinance.nipfp.org.in/PDF/BP2018_Data-localisation-in-India.pdf (Hereinafter 'Parsheera and Bailey) 35

[76] Drawing from Kostov and Schechner's analysis, Parsheera and Bailey state that larger companies found complying with GDPR easier in the short run

[77] Parsheera&Bailey give the example of online gaming sites withdrawing from EU after the implementation of GDPR.

[78] A. Mukherjee, "Protection for Unruly Data," Outlook India, 2 August 2018, <https://www.outlookindia.com/magazine/ story/protection-for-unruly-data/300460>; A. Thaker, India's data localisation plans could hurt its own startups the most, October 16 2018, <https://qz.com/india/1422014/rbis-data-localisation-could-hurt-indias-own-startups/>; V. Kesari, Data localisation and the danger of a 'splinternet', July 26, 2018.

[79] D. Reisman, '*Where is your data, Really?: The Technical Case Against Data Localization*', May 22, 2017, <https://www.lawfareblog.com/where-your-data-really-technical-case-against-data-localization>.

[80] In order to ensure that data reaches the users as fast as possible, data may be kept in select chunks known as "edge caches". Caches allow the most-in-demand content to be located closest to end users who will desire to use it, thereby shortening the distance the data packets have to travel. Thus, the cost of storing all data can be shifted to centralized locations while less expensive machines in different countries can distribute this data to the end user.

Balancing,[81] Data Sharding,[82] back-up in case of software failure,[83] debugging,[84] Reisman argues that the ambiguous locations of data storage make it technically difficult to conceptualize a workable data localisation model.[85] Therefore, the forced splitting of datasets might lead to the creation of vulnerable points, which is compounded by the possibility of error when the prospect of mirroring is introduced.[86]

3. *Experiences in Other Economies*

It is useful to delve into the experience of other economies that have embarked on data localisation to estimate potential impacts of this move on India's innovation economy.In this section we analyze three countries-China (which has a stringent localisation law and an arguably robust innovation economy), Israel (no localisation law and a robust innovation economy) and Russia (localisation law and arguably declining economy) The learnings from these jurisdictions can naturally not be directly transplanted into India but serve as useful flagging devices to determine the potential correlation between localisation and the growth of an Indian indigenous economy.

China

The Srikrishna Report has cited the example of China as an economy being spurred on by AI-driven growth. There were 220 unicorns (startup companies valued in excess of $1 billion) in the world as of 2017, out of which 109 were from the US and China placing a close second with 59, thus clearly outpacing the rest of the world.[87] China

[81] In order to prevent wastage of resources, a web service replicates user data across centres in various regions so that data may be routed to a replica in a different region if a certain region has increased user activity and therefore is unable to meet the demand.

[82] In order to store vast quantities of data, a web service stores data across 'shards', with a single computer holding a shard of data. An individual's data is often split up across a number of shards and backed up on multiple machines. This allows the web service to improve its efficiency by balancing the load based on which 'shards' of data need to be copied and distributed.

[83] Web service providers keep regular back-ups of datasets so that it does not get lost in case a technical failure leads to deletion of the data. Often backups are kept in different regions in order to guard against natural disasters or physical disruptions.

[84] As engineers seek to diagnose and remedy problems that crop up during a product or service's life cycle, engineers often have access to data stored in other jurisdictions for the purposes of such diagnosis and deployment of an appropriate patch.

[85] D. Reisman, '*Where is your data, Really?: The Technical Case Against Data Localization*', May 22, 2017, <https://www.lawfareblog.com/where-your-data-really-technical-case-against-data-localization>.

[86]Cohen, B., Hall, B. & Wood, C., Data localisation laws and their impact on privacy, data security and the global economy. Antitrust, Vol. 32, No. 1, Fall., 2017, <https://www.americanbar.org/content/dam/aba/ publications/antitrust magazine/anti fall2017 cohen.authcheckdam.pdf>

[87] A. McNeice, China's share of the world's billion-dollar startups is growing, October 18 2018, <http://www.chinadaily.com.cn/business/2017-10/18/content_33383247.htm>

also has one of the most stringent localisation mandates in the world, which might inspire economies seeking to cultivate a similarly strong private technology sector into adopting similar mandates.

However, the causal link between data localisation as a policy imperative and China's technology boom is unclear and is not delved into by the Srikrishna Report. This is because there are a host of other factors, independent of the recently imposed localisation mandates, which may have also contributed to the boom. When understanding what benefits localization can bring to a domestic economy, it is important to take into consideration the range of factors that may have led to China's success and evaluate their feasibility in the present Indian economic and political set-up.

First, China has seen a proliferation of home-grown technology combined with local skilling encouraged and boosted by government policy and action. The Make in China 2025 sets out clearly defined and implementable self-sufficiency targets and the methods of attaining them.[88] As part of its economic revitalisation strategy, the Chinese central government announced the Decision on Accelerating the Cultivation and Development of Strategic Emerging Industries in 2010.[89] China has taken active measures to boost indigenous R&D capability, and in 2015, put forward a clear policy that promoted start-ups through the revision of laws and regulations, preferential taxes and support for human resource development and skilling.[90] The Chinese private sector followed suit and began attracting top global talent to China by offering salaries that compete with their Silicon Valley equivalents.[91]

The second crucial factor is the sizeable venture capital funding provided by the Chinese government. In 2016, 35.3% of the venture capital funding in China came from government institutions and state-owned enterprises. In the post-2008 period, the Chinese version of Quantitative Easing (QE) lead to the generation of massive funds that were channeled towards R&D, hiring Chinese and foreign experts and the import of high-tech capital goods.[92] Further, local governments at the province and district

[88] M. Cyrill, What is Made in China 2025 and Why Has it Made the World So Nervous?, December 28 2018, <https://www.china-briefing.com/news/made-in-china-2025-explained/>
[89] K. Fujishiro, Factors Behind Rise In Startups In China, February 2018, <https://www.mitsui.com/mgssi/en/report/detail/__icsFiles/afieldfile/2018/04/20/180216i_fujishiro_e.pdf>
[90] Ibid.
[91] B. O'Keefe, Why China Will Soon Challenge Silicon Valley, July 18, 2018 <http://fortune.com/2018/07/17/china-will-soon-challenge-silicon-valley/>
[92] Y. Li, Understanding China's Technological Rise, August 3 2018, <https://thediplomat.com/2018/08/understanding-chinas-technological-rise/>

level also offer funding opportunities for venture capital. In a typical model, the local government establishes a parent fund, which invests in various industrial funds as a limited partner and then catalyzes the investment process by soliciting funds from various state owned enterprises.[93]

Third, Chinese economic growth, across sectors, lies in the design and implementation of adequate physical and procedural infrastructure for industry to develop. Forced urban planning and zoning of industries across the country lead to the fermentation of business districts that facilitated the congregation of businesses. [94]

It is also important to note that there are certain actions that cannot be directly adapted to an Indian context because of the differences in the social, political and economic framework. Till the introduction of China's Cyber Security Law, China did not have a robust privacy or data protection regime, which could prevent the state from accessing and sharing data with private actors.[95] It is also crucial to note that the market reach of the Chinese tech giants-Alibaba, Tencent or Baidu is largely limited to Chinese consumers. The sheer number of Chinese internet users - over 800 million at the time of publication[96] - enables them to generate enough revenue to place in proximity to, or even above their Silicon Valley counterparts in the global pecking order.[97]

---

[93] K. Fujishiro, Factors Behind Rise In Startups In China, February 2018, <https://www.mitsui.com/mgssi/en/report/detail/__icsFiles/afieldfile/2018/04/20/180216i_fujishiro_e.pdf>

[94] YY Ang, The Real China Model, June 29 2018, <https://www.foreignaffairs.com/articles/asia/2018-06-29/real-china-model>

[95] ("Most of the regulations are aimed at holding companies and individuals—rather than government bodies—accountable for data collection and protection. By contrast, government authorities now have access to more sensitive personal data than ever (through either court orders or surveillance). In addition, law enforcers are requiring companies to ensure a longer period of data retention and zero exemptions from real name registration policies") L Ruan, Big data in China and the battle for privacy, June 22 2018, <https://www.aspi.org.au/report/big-data-china-and-battle-privacy>; China's data protection regime is still yet to take shape and contains amorphous concepts and definitions of concepts. Further, it only places encumbrances on Chinese and foreign companies and does not constrain the government.

[96] N. McCarthy, China Now Boasts More Than 800 Million Internet Users And 98% Of Them Are Mobile [Infographic], August 23 2018, <https://www.forbes.com/sites/niallmccarthy/2018/08/23/china-now-boasts-more-than-800-million-internet-users-and-98-of-them-are-mobile-infographic/#1e6c9ade7092>

[97] The top 8 companies in the world by market value are (in order) Apple, Google, Microsoft, Amazon, Tencent Holdings, Berkshire Hathaway, Alibaba, Facebook; E. Picardo, Eight of the World's Top Companies Are American, February 3 2019, <https://www.investopedia.com/articles/active-trading/111115/why-all-worlds-top-10-companies-are-american.asp>

Finally, assuming that a constitutionally viable data sharing policy was legally and practically feasible, the benefits of sharing data are contested. Ding argues that while China's AI capabilities are only half that of the US, easy access to data gives it a competitive edge in the AI race.[98] On the other hand, Andrew Ng has argued that the benefits of big data may be overstated,[99] since beyond the availability of data, demarcating, picking and operationalizing enough **relevant** data sets is still a challenge.[100] Insiders at Tencent have claimed that the company finds it difficult to integrate various data streams due to various logistic and technical hurdles.[101] **It is crucial to remember that the mere availability of vast quantities of data does not enable AI development. The quality of data, which is a function of research, infrastructure and other factors outlined above are equally important for harnessing that data - for which data localisation is an inadequate stand alone solution.[102]**

Second, a major factor behind the rise of indigenous Chinese companies is simply that most foreign companies were banned,[103] supposedly to preserve social stability, [104] from the Chinese market.[105] Finally,this, coupled with a smooth regulatory landscape enabled the cultivation of rising giants in a variety of sectors each feeding off the benefits of a captive 800 million strong internet using population.On the other hand, India has a significantly lower internet user base of 500 million. It is also

---

[98] J Ding., Deciphering China's AI Dream, March 2018, <https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf>

[99] S. LeVine, Axios Future Newsletter, October 18 2018, <https://www.axios.com/newsletters/axios-future-5443c000-9035-4915-8924-6158c6a37bf7.html?chunk=0&utm_term=emshare#story0>

[100] D. Pereira, Andrew NG's "The State of Artificial Intelligence" reviewed, January 9 2018, <https://medium.com/@dpereirapaz/andrew-ngs-the-state-of-artificial-intelligence-reviewed-7007d95a72a1>

[101] R. Zwetsloot, H. Toner, and J. Ding, Beyond the AI Arms Race, November 16 2018, <https://www.foreignaffairs.com/reviews/review-essay/2018-11-16/beyond-ai-arms-race>

[102] IBM estimates that 80% of available data is dark to most companies as they are unstructured and therefore cannot be used as training sets for algorithms delving into predictive analytics. See B Kristifoe,"Marketing in the dark-Dark Data",2018,https://www.ibm.com/blogs/think/be-en/2018/04/24/marketing-dark-dark-data/

[103] L. Yuan, A Generation Grows Up in China Without Google, Facebook or Twitter, August 6, 2018, <https://www.nytimes.com/2018/08/06/technology/china-generation-blocked-internet.html>

[104] The Economist, How does China censor the internet?, April 22 2013, <https://www.economist.com/the-economist-explains/2013/04/21/how-does-china-censor-the-internet>

[105] Towards the end of the 2000s as China acquired a virtual monopoly in the supply chain of high-tech goods and increased its political and financial capital, it shifted its economic strategy from seeking investment from western firms to slowly displacing them. M Stoller, If the U.S. Doesn't Control Corporate Power, China Will, October 11 2018, <https://foreignpolicy.com/2018/10/11/if-the-u-s-doesnt-control-corporate-power-china-will/>

important to note that China is a far more urbanised nation[106] with a far higher GDP per capita.[107] The affluence of the user impacts the extent to which revenue can be generated by processing that data. A rural internet user is unlikely to use or generate data that could be revenue-generating for tech start-ups most of which focus on homogenous consumption patterns of the urban population. Food delivery services, ride-sharing apps or online ticketing and shopping services are unlikely to be consumed or used by the next generation of users in rural India.[108] This explains why several start-ups sought to expand their business to overseas markets in 2018 as the Indian market was saturated after their initial urban foray.[109] AliBaba and Tencent continue thriving from the data generated by Chinese users but it is unlikely that an Indian start-up will be able to do the same only with data generated by Indian users.

Israel

On the other hand, Israel is a model for start-up incubation that has thrived without any sort of data localisation. Israel has 7,000 start-ups, 350 VC funds and over 300 corporate R&D centres.[110] Israel does not have any policy that restricts the cross-border flow of data in place. However, just as in the case of China, the thriving tech sector in Israel may owe more to factors other than a mere lack of restriction on cross border flow of data. As argued by Senon and Singer, the growth in the tech sector in Israel has hinged around[111] :

1. **Education and Research:** The government spends 4.3% of its GDP on Research & Development while India spends just 0.8%.
2. **Immigration:** Senon and Singer believe that the work ethic and risk-taking drive in migrants has further propelled the start-up economy.
3. **Government support and enabling ecosystem:** The Israeli Government plays a vital role in the startup and innovation ecosystem, both directly and indirectly.

[106] 57.96% of China's population is urbanised with a total of 1.39 million people living in cities. India is only 33.60% urbanised. UN DESA, 2018 Revision of World Urbanization Prospects, May 16 2018, <https://www.un.org/development/desa/publications/2018-revision-of-world-urbanization-prospects.html>

[107] https://www.cia.gov/library/publications/the-world-factbook/rankorder/2004rank.html

[108] S. Tandon, India's rural internet users love Facebook, WhatsApp and free music downloads, August 12, 2016 <https://qz.com/india/755825/anatomy-of-a-rural-internet-user-in-india/>;https://factordaily.com/indian-ai-has-a-dataset-problem/

[109] A.Bhattacharya,2018 was the year India's startups decided to go global,https://qz.com/india/1490980/ola-oyo-byjus-swiggy-made-2018-indian-startups-global-year/

[110] A. Paranjape, Israel – 'The Startup Nation', Lessons For India, February 11 2018, <https://swarajyamag.com/science/israel-the-startup-nation-lessons-for-india>

[111] D. Senor and S. Singer(2011), *Start-up Nation: The story of Israel's economic miracle*

Directly, it supports 19 entrepreneurship programs, funds, and incubators.[112] The incubators provide capital, facilities and risk assessment to universities and professors who are able to use them to propel their start-ups. The government prioritises start-ups looking for innovative solutions in critical areas such as agriculture, water supply and defense.

Russia

Russia is an example of a country whose economy has suffered possibly from the impacts of data localisation. As per an ECIPE report,[113] data localisation may lead to productivity losses for domestic firms as they might be unable to use services from abroad, or may be compelled to set up a data centre within Russian territory. Analogous experiences in the past suggest that the data-intensive service industry will shift costs that emerge from regulatory compliance to other sectors of the economy. Further, the productivity losses will likely result in lowered investment and higher prices of imports. The losses are equivalent to 0.27% of gross domestic product (GDP), equivalent to a loss of 286 billion roubles (US$ 5.7 billion). Applied with 2015 IMF forecasts, the Russian economy was predicted to contract by 4.1% in 2015. It contracted by 2.5% in 2015 and a further 0.2% in 2016, although this might have been the product of other geo-political shocks such as the imposition of sanctions. [114]

Enhancing National Security and Law Enforcement Access

Law Enforcement Access

Access to data by domestic law enforcement authorities is important. As recognised by the Srikrishna White Paper, a disproportionate amount of data associated with Indian citizens is stored in the United States. The presently existing Mutual Legal Assistance Treaties process (MLATs) through which Indian law enforcement authorities gain access to data stored in the US is excessively slow and cumbersome. The White Paper goes on to propose data localisation as a solution to ensuring access by law enforcement. Yet, it is important to realize that even if data is stored in

[112] A. Paranjape, Israel – 'The Startup Nation', Lessons For India, February 11 2018, <https://swarajyamag.com/science/israel-the-startup-nation-lessons-for-india>
[113] M. Bauer, H. Lee-Makiyama, E van der Marel, Data Localisation in Russia: A Self-imposed Sanction, June 2015, <http://ecipe.org/publications/data-localisation-russia-self-imposed-sanction/>
[114] As noted above, we do not necessarily agree with the assumptions and statistical extrapolations made in the ECIPE papers but as we did not conduct empirical research ourselves, we have quoted the numbers. Readers are encouraged to peruse the reports we quoted carefully to make an independent assessment.

India as per the draft Personal Data Protection Bill, challenges may still exist. Namely:

1. First, as recognised by the report of the Committee, a conflict of law question may still arise despite the data being physically stored in India. This could be the case as the country where the mirror copy is stored will retain its right to assert territorial jurisdiction. In most cases, this is also where the data processor, usually a Multinational Corporation is incorporated. This might mean that if Twitter or Facebook handed over the physical copy of data stored on Indian servers to Indian law enforcement authorities, they could be challenged in a U.S. court if they did not comply with U.S. law while doing so. **Therefore, with respect to disclosure, unless the individual that the data pertains to is a resident of a country, the servers are located within the same country, and the company is incorporated within the same country - disclosures will potentially be governed by the laws of at least two countries-leading to a conflict of laws scenario and greater uncertainty.**[115]

2. The Srikrishna Report seems to assert that foreign entities may be less likely to refuse access to data if the data is stored in India, as India would have a stronger claim in International Law and also help make a case for any conflict to be resolved by an Indian court. While this assertion may be theoretically probable, there is no evidence to suggest that a stronger position in International Law will necessarily foster better compliance by foreign companies. Instead, India would fare better if it were to use the language of international law to articulate its position in the MLAT reform process,[116] or to propel itself to a better position under the CLOUD Act (which requires countries to demonstrate a commitment to a free and open internet)[117] or potentially pursue negotiations for a multilateral data sharing treaty.

3. The localisation mandate proposed in the Bill only extends to data relating to Indian citizens. It does not solve the problem, that arose in the

[115] D. Castro, The False Promise of Data Nationalism, December 2013, <http://www2.itif.org/2013-false-promise-data-nationalism.pdf>
[116] A. Sinha, and ors., Cross Border Data-Sharing and India, Centre for Internet and Society, 2018 <https://cis-india.org/internet-governance/files/mlat-report>
[117] E. Hickok, and V. Kharbanda, An Analysis of the CLOUD Act and Implications for India, Centre for Internet and Society, 2018 <https://cis-india.org/internet-governance/blog/an-analysis-of-the-cloud-act-and-implications-for-india>; See also "Promoting Public Safety, Privacy and the rule of law around the world: The Purpose of the CLOUD Act" <https://www.insideprivacy.com/cloud-computing/department-of-justice-releases-white-paper-on-cloud-act/>

Microsoft-Ireland case[118] where law enforcement agencies required access to data relating to a foreigner in a server located in another jurisdiction but by a company incorporated in the US.

There are several examples of other measures that are being deployed to attain the same objectives, which India could emulate. For example:

Europe E-Evidence Directive

The European Commission proposed draft legislation on e-Evidence (both a Regulation and Directive) in April 2018 to facilitate cross-border data-sharing in the case of criminal investigations. As per the legislation, law enforcement authorities across EU member states can compel "production orders" from communication and cloud-based service providers inside or outside the EU regardless of where the data is located. The Directive further requires EU member states to establish legal representatives for the receipt of cross-border demands. Taken together, the Regulation and Directive would effectively give EU member states access for law enforcement purposes to the data of internet users not only across the EU, but worldwide. The EU's e-Evidence proposal, importantly, focuses on access, not location, and provides another potential model for addressing the law enforcement access problem in India.

U.S. CLOUD Act

The Clarifying Lawful Overseas Use of Data Act or CLOUD Act (H.R. 4943) is a United States federal law enacted in 2018 that adapted existing privacy standards to modern day requirements such as cloud computing.[119] The CLOUD Act allows the U.S. government to enter into bilateral agreements with other countries that have adequate standards to ensure the safeguarding privacy, human rights and due process. The CLOUD Act therefore provides a mechanism that allows for the resolution of conflict of laws issues and enables law enforcement access to data whenever needed.

[118] A. Basu, The Microsoft-Ireland Ruling is a game changer for data protection and #MLAT regimes, July 18 2016 <https://www.orfonline.org/expert-speak/the-microsoft-ireland-ruling-is-a-game-changer-for-data-protection-and-mlat-regimes/>

[119] K. Houser, Everything You Need to Know About the CLOUD Act, March 26 2018, <https://futurism.com/everything-need-know-cloud-act>

Protecting Against Foreign Surveillance

The Srikrishna Report argues that given the strategic and economic interests in personal data, it must be protected against foreign surveillance. It raises the concern that a large number of information intermediaries such as Google, Facebook, Amazon, are headquartered in the United States and may be compelled by US law such as the PATRIOT Act or the Foreign Intelligence Surveillance Act (FISA) to conduct surveillance on Indian citizens[120] However, the Committee recommends against processing data exclusively in India, as it would result in an Indian internet walled away from the rest of the internet. Thus, it recommends that data which may be of heightened national interest must be processed exclusively in India. It presents examples of critical data such as Aadhaar data, genetic data, biometric data and health data.[121]

However, there may be some issues with such a proposition. First, the Draft Bill allows for personal data (other than critical data) to be mirrored in other jurisdictions. The localization mandate thus does not address surveillance concerns with regard to such data. With respect to critical data that must be stored exclusively within India, such a policy may reduce the quality of security provided by local service providers depending on national requirements and enforcement of the same. [122] Further, having localized data servers reduces the opportunity to keep the data in motion across multiple locations through sharding, as the architecture of the internet enables companies to do so. By compelling the storage of data in a few physical data centres,the local storage requirement offers a potential honeypot opportunity for both criminals and foreign intelligence agencies alike.[123] Further, it shifts the burden onto the Indian government and security providers to guarantee the physical security of the established structure.

Internet governance pundit and Executive Director of CIS,Sunil Abraham refers to this phenomenon as a 'regulatory stretching of the attack surface'[124]-where regulation is

[120] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, <https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf>
[121] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, <https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf>
[122] A Chander and U.Le, "Breaking the Web: Data Localisation v the Global internet" <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858>.
[123] Kuner, C., Data nationalism and its discontents. 64 Emory Law Journal Online 2089., 2015, <http://law.emory.edu/elj/elj-online/volume64/responses/data-nationalism-its-discontents.html>.
[124] Personal interview

enabling the osmosis of vulnerabilities both in the physical data centres and the security architecture of the internet-thereby artificially stretching the window of opportunity or the attack surface for potential adversaries.

Threat to fibre-optic cables

The Srikrishna Committee report cites studies which suggest that undersea cable networks that transmit data from one country to another are vulnerable to attack. Therefore, it argues that processing critical data on Indian territory would minimise the vulnerability of relying on undersea cables. It cites a report by Policy Exchange that states that the threat to undersea cables by Russian actors may be an existential one for the UK.[125] However, it does not engage with the solutions offered by the same report, which largely suggest improving the UK's defense and security posture and co-operating with global partners and allies to protect these underwater cables.[126] The recommendations offered by the report for developing United Kingdom's strategy in this domain include :

- Undertake a large scale strategic review that maps risks to this infrastructure and identify steps that UK has taken to mitigate these risks
- Update the National Risk Assessment and Risk Register
- Secure landing sites
- Establish Cable Protection Zones (CPZ) in collaboration with international partners in areas with high value communication corridors, not only around the UK but also in strategic geo-strategic nodes such as the Mediterranean and the Suez
- Improve the quality of equipment deployed on cables
- Work with the private sector to increase the geographic diversity of undersea cables by increasing the number of landing sites, thus averting over-reliance on a few choke points
- Encouraging the private sector to build back-up cables

[125] R. Sunak MP, Undersea Cables, Policy Exchange, 2017, 5 <https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf>

[126] The recommendations offered by the report for developing United Kingdom's strategy in this domain include: (i) Undertake a large scale strategic review that maps risks to this infrastructure and identify steps that UK has taken to mitigate these risks (ii) Update the National Risk Assessment and Risk Register (iii) Secure landing sites (iv) Establish Cable Protection Zones (CPZ) in collaboration with international partners in areas with high value communication corridors, not only around the UK but also in strategic geo-strategic nodes such as the Mediterranean and the Suez (v) Improve the quality of equipment deployed on cables (vi) Work with the private sector to increase the geographic diversity of undersea cables by increasing the number of landing sites, thus averting over-reliance on a few choke points (vii) Encouraging the private sector to build back-up cables (viii) Working to improve the piecemeal International Law regime securing undersea cables.

- Working to improve the piecemeal International Law regime securing undersea cables.

These suggestions, rooted in international diplomacy and security measures are valuable lessons for India as well. India will need to conceptualize beyond localization and consider vulnerabilities in the transport - sea-cables[127], for example. Further, a comparative assessment of the risks posed by the transport (sea cables, etc.) and storing data on servers in India needs to be undertaken.

Data Protection and Enforcement

The Srikrishna Report cites enforcement of domestic laws generally, and data protection laws in particular, as a key justification for mandating local storage of data.[128] It argues that "effective enforcement of data will invariably require data to be locally stored within the territory of India," and that the local storage of data is intrinsically connected to the enforcement of domestic law.[129]

At the outset, it must be noted that given territorial limitations, ensuring effective enforcement jurisdiction is a concern that is not limited to data protection, but applies to all online activity. With respect to data protection, various models may be considered that do not require compliance with local storage mandates. For instance, under the EU's GDPR, adequacy assessments (which allow unrestricted cross-border transfers) evaluate whether sufficient redressal mechanisms are accessible to data subjects, when data is processed outside the European Union.[130] Other methods that allow cross-border transfers under the GDPR, such as the standard contractual clauses, also incorporate such conditions.[131]

[127] G. Hinck, Evaluating the Russian Threat to Undersea Cables, March 5, 2018 <https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables>
[128] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, <https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf>
[129] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, <https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf>
[130] Recital 104, GDPR.
[131] Recital 108, GDPR.

Another approach, as exemplified by the EU's e-evidence directive,[132] as well as the GDPR,[133] is the requirement for designating a legal representative in the Union for the receipt of, compliance with and enforcement of decisions and orders. As a note, the proposed Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018[134] incorporate a similar requirement, wherein certain categories of online intermediaries must (i) incorporate in India under the Companies Acts, 1956 or 2013; (ii) have a permanent registered office in India; (iii) appoint a representative in India to coordinate with law enforcement, and ensure compliance with orders and requisitions.[135]

Widening Tax Base

Another reported justification for data localisation is to ensure that certain multi-national corporations come within the Indian tax regime for, inter alia, services sold to Indian citizens.[136]The concerns within government stems from the fact that these entities offer services without having a presence in India and only entities present in India can be taxed as per present Indian laws.[137]

When considering data localization as a solution for this concern, it is important to consider other alternatives that exist. India has already begun working towards taxing digital transactions through the introduction of an Equalisation Levy (EL) since June, 2016 on online advertisements as part of The Finance Act.[138] As of now the

[132] Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings COM/2018/226 final - 2018/0107 (COD)
[133] Article 27, GDPR.
[134] The Information Technology, [Intermediaries Guidelines (Amendment) Rules], 2018, <https://meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf>
[135] Clause 7, Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018.
[136] Agarwal S and Mandavia M, Local servers of tech giants like Facebook, Google may help Indian govt debit taxes, 2018, <https://tech.economictimes.indiatimes.com/news/corporate/local-servers-of-tech-giants-like-facebook-google-may-help-indian-govt-debit-taxes/67121194>
[137] Ibid.
[138]The Gazette of India, Extraordinary, Part II, dated May 14, 2016. <http://www.cbec.gov.in/resources//htdocs-cbec/finact2016.pdf> V. Vasal, Evolution of digital economy and taxation challenges, October 13 2018, <https://www.livemint.com/Politics/7fPthmfawKPnhF2IsufkmL/Evolution-of-digital-economy-and-taxation-challenges.html> , See A. Lahiri, "Equalisation Levy", 2017 <https://www.brookings.edu/wp-content/uploads/2017/01/workingpapertax_march2017_final.pdf>

equalisation levy stands at 6%.[139] This levy is applicable for any consideration received or receivable by non-residents providing the following B2B services[140]:
(a) Online advertisement
(b) Any provision of digital advertising space
(c) Any facility or service for online advertisement
(d) Any other service that can be notified later.

While there are several concerns around the imposition of an equalisation levy, lessons-both positive and negative from across the world can be studied to incorporate a model that works for the present circumstances of India's digital economy.[141]

The Finance Act, 2018 brought in the concept of Significant Economic Presence (SEP) in Section 9 of the Income-tax Act, 1961 (the Act). It stated that the SEP of a non-resident in India will constitute its business connection in India. For this purpose, SEP has been defined as the following:

(a) A transaction in respect of any goods, services or property, including provision of downloaded data or software, carried out by a non-resident in India if the aggregate of the payments arising from such transactions during the previous year exceeds the prescribed threshold

(b) Systematic and continuous soliciting of business activities or engagements involving interaction with the prescribed number of users in India using digital processes

On 14 February the Central Board of Direct Taxes (CBDT) introduced a draft proposal that would mandate a 30% tax on Indian companies while subsidiaries of foreign companies will have to pay 30% tax based on the revenues and user base of these companies.[142]

[139] Ibid
[140] Ibid
[141] Katie, "Digital Taxes Around the World: What to Know about new tax rules", 2019 <https://quaderno.io/blog/digital-taxes-around-world-know-new-tax-rules/>
[142] S. Choudhary, "Google, Facebook, Twitter, Amazon stare at 30-40% digital tax blow in India", 2019, <https://www.business-standard.com/article/companies/google-facebook-twitter-amazon-stare-at-digital-tax-of-30-40-in-india-119021401356_1.html>

While an equalisation levy has come under some criticism[143] and is certainly not a 'one-stop' solution for tax evasion, it demonstrates that there are different policy levers that can be leveraged to ensure that companies are appropriately taxed under national taxation laws. The projected costs and benefits of each policy measure needs to be closely assessed before using data localisation as a prescription for ensuring that foreign companies are appropriately taxed. .

Data Sovereignty and India's Trade Commitments

Data localization measures can have implications beyond the immediate national impact and can extend to a country's international relations and associated agreements and relationships. For example, data localization measures could have implications for India's trade commitments--something that will be useful for the Ministry of Commerce and Ministry of External Affairs to be cognizant of. While restrictions on the free flow of data has not yet been challenged in any global forum, we map certain provisions in the World Trade Organization (WTO) framework that might come into play and project potential consequences on India's negotiating position in other fora such as the Regional Comprehensive Economic Partnership if comprehensive data localization requirements are put in place. These include:

World Trade Organization Framework: Implications for the General Agreement on Trade in Services

When the World Trade Organisation (WTO) was created, the existing General Agreement on Tariffs and Trade (GATT) was revised and juxtaposed with an array of agreements that would enlarge the scope of the rules based order governing international trade.[144] As the GATT was restricted to governing trade in goods, WTO members felt that it was necessary for them to sign a new agreement to also cover trade in services. This agreement was called the General Agreement on Trade in Services (GATS). Although some authors have argued that data may fall within the ambit of GATT[145], it has been demonstrated that doing so would encompass a smaller

[143] OECD, "Tax Challenges arising from Digitisation: Interim Report", 2018, <https://www.oecd-ilibrary.org/docserver/9789264293083-en.pdf?expires=1551352720&id=id&accname=guest&checksum=C6D530B6C4C3A8B5C566AE2F01A8136D>

[144] World Trade Organization (WTO): Documents Online. <https://docs.wto.org/dol2fe/Pages/FE_Browse/FE_B_009.aspx?TopLevel=3875#/>

[145] MARA BURRI, The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation, 51 U.C. DAVIS L. REV. 65 (2017).

range of companies than GATS, as certain types of data might not be considered a good.[146]

Much like the GATT, the GATS aims at protecting competitive opportunities for companies across the globe regardless of the origin of their services and endeavours to achieve progressive liberalisation of service of the market for services.[147] The broad approach and structure of the GATS is different from the GATT as the object of regulation is services and not goods.[148] The GATS is a holistic agreement that covers all service sectors barring those services "*supplied in the exercise of governmental authority.*"[149]

Like the GATT, there are two core obligations in the GATS.[150] The Most Favoured Nation (MFN) clause enshrined in Article II:1 obliges Member States to "accord immediately and unconditionally to services and service suppliers of any other Member treatment no less favourable than that it accords to like services and service suppliers of any other country."

However, unlike the GATT, the MFN obligation in GATS allows for some flexibility in complying with this obligation. Each member may specify which measures the MFN obligation would not apply to as long as said measures are listed in and meet the conditions laid out in the opt out' on Annex II exemptions.[151] The MFN obligation is supplemented by certain positive commitments put forward by individual members that are listed in the appended "Schedules of Specific Commitments."

These positive commitments codify the following obligations that each member takes upon themselves[152]:

---

[146] For example Data as a service Daas companies) J. Meltzer, The Internet, Cross-Border Data Flows and International Trade, February 2013, <https://www.brookings.edu/wp-content/uploads/2016/06/internet-data-and-trade-meltzer.pdf>
[147] Brown CA. Non-discrimination and Trade in Services. Springer; 2017.
[148] Sandra Anderson, General Agreement on Trade in Services: A Resource for Librarians, U. OF ALTA., <http://capping.slis.ualberta.ca/global/sandra/history.html>.
[149]GATS art. I, ¶ 3(b). Paragraph (c) clarifies that "'a service supplied in the exercise of governmental authority' means any service which is supplied neither on a commercial basis, nor in competition with one or more service suppliers." Id. art. I, ¶ 3(c).
[150] M. Matsushita, "Basic Principles of the WTO and the role of competition policy", 2004, <https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1247&context=law_globalstudies>
[151] Broadman, Harry G. "International Trade and Investment in Services: A comparative Analysis of the NAFTA." In *Int'l L.*, vol. 27, p. 623. 1993.
[152] Burri, Mira. "The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation'(2017)." *UC Davis Law Review* 51: 65-85.

1) **“Market access”** which is provided for in Article XVI GATS and incorporates obligations relating to quantitative restrictions to trade in services
2) **The “national treatment” obligation,** enshrined in Article XVII GATS which bans discrimination between domestic and foreign services and service suppliers. In practice, the Members’ schedules of commitments represent a codification of the market access conditions which foreign service providers can rely on with some certainty.[153]

The services sectors that are relevant for the digital economy including telecommunications, the computer and related services, the audiovisual, as well as the financial services sectors. GATS Article I:2 states the definition of cross-border “trade in services,” as , in part, providing a “cross border supply” of a service from a provider located in “the territory of one Member into the territory of any other Member.” Therefore, data transfers and digital transfers are said to broadly fall under this provision of the GATS.[154]

There are four modes of providing services under the GATS[155]:

Mode 1:Cross-border:Services supplied from the territory of one member into the territory of any other Member.

Mode 2:Consumption abroad:Services supplied in the territory of one member to the service consumer of any other Member

Mode 3:Commercial presence: Services supplied by a service supplier of one member, through commercial presence, in the territory of any other.

Mode 4:Presence of natural persons: Services supplied by a service supplier of one Member, through the presence of natural persons of a Member in the territory of any other Member

The types of “service[s]” utilized for data transfer are further clarified in the Scheduling Guidelines, which provide that protections for cross-border supply of services apply to service providers “not present within the territory of the Member” and “service delivered within the territory of the Member from the territory of

[153] Ibid.
[154] Ibid.
[155] Broadman, Harry G. "International Trade and Investment in Services: A comparative Analysis of the NAFTA." In *Int'l L.*, vol. 27, p. 623. 1993.

another Member."[156] This would likely be characterized as a mode 1 service transfer which has potential implications for the proper regulation, market access and national treatment obligations contained in GATS.

GATS Article VI-Proper Regulation

Under GATS Art VI:1, the GATS states that all members must "ensure that all measures of general application altering trade in services are administered in a reasonable, objective and impartial manner." GATS Art VI:5(a) refers to GATS Art VI:4 must ensure that "licensing requirements and technical standards" do not nullify or impair the commitment made in the schedule of commitments and therefore make it more burdensome than necessary to guarantee the quality of the service. Commitment to the GATS does not leave member state with a broad discretion on restricting data flows. [157]

GATS Art XVI-Market access

GATS Art XVI charts out market access obligations that apply based on the commitments made by a member in the schedule regarding the concerned mode and service sector in question. Unless appropriate limitations or pre-conditions have been carved out in the schedule itself, any member that has made a market access commitment cannot limit the number of service suppliers or the total number of service operations or the total quantity of service output. With regard to restraints on data flows, the Appellate Body stated in *US-Gambling* that a ban on the remote supply of betting and gambling services via online platforms operated as a zero quota which would violate the requirements of this article.[158]

GATS Art XVII-National Treatment

The fundamental principles of free and fair international trade stem from the doctrine of national treatment. Article XVII of the GATS incorporates the national treatment rule into its tapestry. [159]It compels members to provide equal market

[156] J Blum,"Reading the Trade Tea Leaves: A comparative analysis of potential US WTO-GATS claims", 2018,
<https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/08/GT-GJIL180026.pdf>
[157] Mitchell, A. D., & J. Hepburn, Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer, Yale JL & Tech., 19, 182.
[158] Appellate Body Report, United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services, ¶ 95, 294, 296, 301, 313, WTO Doc. WT/DS285/AB/R (adopted Apr. 7, 2005)
[159] J. Blum, "Reading the Trade Tea Leaves: A comparative analysis of potential US WTO-GATS claims", 2018,
<https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/08/GT-GJIL180026.pdf>

access to foreign and domestic service providers for all services listed in the schedule. Crucially for digital trade,footnote 10 specifies that member cannot use provisions to compensate for " any inherent competitive disadvantage, which results from the foreign character of the relevant services or service suppliers." While 'likeness of a service' is important for the national treatment requirement to apply, the sheer scale of the digital economy means that there will be enough characteristics between various types of data to achieve the requisite quantum of likeness.[160]

Art. XIV Exceptions

It is also crucial to note that even if a violation of one of the aforementioned provisions occurs, the general exceptions clause contained in Article XIV of GATS may render the action non-violating.[161] Much like the GATT, to validly fall within the scope of an exception, an action must fall within the ambit of one of the sub-clauses and also satisfy the two-pronged test of the chapeau of Article XIV i.e. not constitute an unjustified or arbitrary restriction or a disguised restriction on trade in services. [162]

The general exceptions contained in GATS Article XIV include measures that are 'necessary' (i.e. there are no less trade restrictive or more WTO compliant alternatives available[163]) for:
(i) Public morals or public order
(ii)Animal, plant life or health
(iii)Prevention of deceptive and fraudulent practices
(iv)Protection of privacy of the individual
(v)Safety

GATS Article IV bis contains exceptions on the grounds of national security which prevent a country from being compelled to furnish information contrary to its essential security interests.

[160] OECD, "DIgital Trade and Marker Openness", 2018 <http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2018)3/FINAL&docLanguage=En>
[161] G. Ayres & A. Mitchell, General and Security Exceptions under the GATT and GATS, in INTERNATIONAL TRADE LAW AND WTO ch. 9 (Indira Carr, Jahid Bhuiyan & Shawkat Alam eds., 2012).
[162] L. Bartels, The Chapeau of the General Exceptions in the WTO GATT and GATS Agreements: A Reconstruction, 109 AM. J. INT'L L. 95 (2015).
[163] Appellate Body Report, China - Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products, ¶ 141, WTO Doc. WT/DS363/AB/R (adopted Dec. 21, 2009), 29.

States have used this criteria to state the objectives of their localisation measures. Russia has justified its law on the lines of security[164] whereas China has cited public morals.[165] Given that any localisation mandate opens India up to challenge at the WTO, any localisation framework, if pursued, should be devised keeping these exceptions in mind with enough evidence to justify their inclusion under the ambit of a stated exception.

Regional Trade Agreements

Two emerging regional trade agreements with opportunities for India include the Regional Comprehensive Economic Partnership (RCEP) and the Free Trade Area of the Asia-Pacific (FTAAP)[166] The RCEP includes ten ASEAN member nations and other countries which have entered into previous agreements with ASEAN countries.[167] China is a part of these negotiations and can be expected to block any attempt at carving out a prohibition on data localization laws-as can Malaysia, Vietnam and other ASEAN countries with domestic data localization laws.[168]

The FTAAP is at an even more nascent stage-arising out of the likely failure of the Trans-Pacific Partnership due to the withdrawal of the US. Given that Russia and China are negotiating members of the FTAAP, it is quite likely that the members

---

[164] Undang-Undang Tentang Pelayanan Publik [Public Service Law Number 25/2009], No. 25/2009, art. 21 (July 18, 2009) (Indon.), http://www.ilo.org/dyn/ natlex/natlex4.detail?p_lang=en&p_isn=84185 [https://perma.cc/YF77-N982]; quoted in Mitchell A and Mishra N (2018)." Data at the docks: Modernizing International Trade Law for the Digital Economy" 20 Vand J Ent&Tech law 4, available at http://www.jetlaw.org/wp-content/uploads/2018/06/3_Mitchell-Article_Final-Review-Complete.pdf

[165] See, e.g., Jisuanji Xinxi Wangluo Guoji Lianwang Anquan Baohu Guanli Banfa (计算 机信息网络国际联网安全保护管理办法) [Measures for Security Protection Administration of the International Networking of Computer Information Networks] (promulgated by the Ministry of Pub. Sec., Dec. 11, 1997, effective Dec. 30, 1997) WIPO, art. 4 (China), <http://www.wipo.int/wipolex/en/details.jsp?id=6571> [https://perma.cc/W8CU-33RD]; Broadcasting (Class License) Notification (Cap 28, N 1, 2004 Rev Ed), Schedule, §§ 13, 15 (Sing.) <https://sso.agc.gov.sg/SL/BA1994-N1?DocDate=20161227> [https://perma.cc/8UXJ-AAV2] quoted in A Mitchell and N Mishra, "Data at the docks: Modernizing International Trade Law for the Digital Economy", 20 Vand J Ent&Tech law 4, 2018, <http://www.jetlaw.org/wp-content/uploads/2018/06/3_Mitchell-Article_Final-Review-Complete.pdf>

[166] John Selby; Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?, *International Journal of Law and Information Technology*, Volume 25, Issue 3, 1 September 2017, Pages 213–23.

[167] Nataraj G and Sahdev G, "RCEP: India must stop being a naysayer", <https://www.thehindubusinessline.com/opinion/rcep-india-must-stop-being-a-naysayer/article25933654.ece>

[168] John Selby; Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?, *International Journal of Law and Information Technology*, Volume 25, Issue 3, 1 September 2017, Pages 213–23

would come out in support of data localization given the significance of both the said economies in these agreements.[169]

EU-India FTA

In the aftermath of Brexit, it has been reported that[170] the European Union (EU) may be reworking the proposed free trade pact with India —called the Broad Based Bilateral Trade and Investment Agreement (BTIA).[171] The negotiations have stagnated over a period of 11 years.[172]

In a strategy paper for India released on Tuesday, the EU did not mention BTIA, but indicated a desire to negotiate a “balanced, ambitious and mutually beneficial" free trade agreement (FTA) with India. A mandatory data localisation provision might be an obstacle as India embarks on these negotiations.

US-India bilateral ties

The prospect of data localization has already come up as an issue in the Indo-US trade relationships as negotiators got into talks to review India’s eligibility under the Generalised System of Preferences (GSP) that allows India to export around 2,000 product lines under ‘zero tariffs.’[173] On March 4, 2019, US President Donald Trump revoked India’s developing country status under the GSP.[174]

A Survey of Stakeholder Responses

In order to further analyse perspectives and reasons on both sides of the localisation debate, we studied the publicly available responses of fifty-one relevant

[169] This reality is very different from the rules being crafted in new NAFTA with Canada, Mexico and USA on board. One provision clearly states “ “No Party shall require a covered person to use or locate computing facilities in that Party’s territory as a condition for conducting business.” “
[170] PTI, “EU unveils strategy paper for ramping up ties with India”, 2018, <https://www.livemint.com/Politics/JY4QUB1YyTgnqdFHMFWyuO/EU-unveils-strategy-paper-for-ramping-up-ties-with-India.html>
[171] Dave D, “Bilateral Trade Investment Treaty: A Complex Treaty between India and EU”, 2017, <https://qrius.com/bilateral-trade-investment-agreement-btia-complex-treaty-india-eu/>
[172] A Sen, “India-EU attempt to restart free trade talks stumbles on old issues”, 2018, <https://www.thehindubusinessline.com/economy/india-eu-attempts-to-re-start-free-trade-talks-stumble-on-old-issues/article25692022.ece>
[173] Hindu Editorial, “No zero-sum games: On India-US trade hostilities”, 2019, <https://www.thehindu.com/opinion/editorial/no-zero-sum-games/article26231336.ece>
[174] A Panda,”Trump announces decision to revoke India’s GSP Status”, 2019,https://thediplomat.com/2019/03/trump-announces-decision-to-revoke-indias-developing-country-gsp-status/

stakeholders to the Draft Personal Data Protection Bill, 2018 released by the Srikrishna Committee. The findings are detailed in **Annex 2.**

Most civil society groups-both in India and abroad were against blanket data localisation, as mandated by the Srikrishna Bill. A variety of reasons were provided-which included high compliance costs, restricting India's access to the internet; no economic or SWOT (Strength Weaknesses Opportunities Threat) analysis being conducted; vague definitions in the text of the bill; and a hindering of innovation. Foreign companies such as Google and Facebook, politicians including US Senators, transnational advocacy groups such as the US-India Strategic Partnership Forum, were against localisation citing it as a grave trade restriction and an impediment to a global digital economy which relies on the cross-border flow of data. The stance companies such as Google and Facebook comes as no surprise, since they would likely incur huge costs in setting up data centres in India if the localisation mandate was implemented.

Stakeholders arguing for data localisation included politicians and some academic and civil society voices that view this measure as a remedy for 'data colonialism' by western companies and governments. Large Indian corporations, such as Reliance, that have the capacity to build their own data centres or pay for their consumer data to be stored on data servers support this measure citing the importance of 'data sovereignty' and to prevent 'data colonisation.'However, industry associations such as NASSCOM and Internet and Mobile Association of Indian (IAMAI) are against the mandate citing a negative impact on start-ups that may not have the financial capacity to fulfil the compliance costs required. Leading private players in the digital economy, such as Phone Pe and Paytm support the mandate on locally storing payments data as they feel it might improve the condition of financial security services.

It is important to note that Chinese players such as Alibaba and Xilinx have come out in favour of this move, possibly because they have already set up a number of data centres across India.

Data Localisation Around the World

As noted earlier, various countries have begun to implement restrictions on the cross-border flow of data. We studied 18 countries that have such mandates and found that models can differ in the strength of the mandate, the type of mandate, the

type of data to which the restriction applies, and sectors to which the mandate extends.

Starting with the **strength of mandate**, we found that some countries (such as China, Nigeria, Russia) have unconditional restrictions on the flow of data outside their territory -i.e- there can be no scenario in which the data under the restricted mandate can flow out. This is in line with China and Russia's stance at the United Nations and other global norms formulation processes, where they have advocated for 'information sovereignty' and the safeguarding of data within their network frontiers.[175] The second group of countries we studied also have an unconditional mandate, but this mandate is restricted to a certain sector. For instance, tax records in New Zealand and sensitive and personal health data in Australia. The final group of countries have a conditional localisation mandate. Some Latin American countries such as Argentina and Colombia, allow for the transfer of data only if the recipient country has an 'adequate data protection framework' in place. This can be interpreted as a local storage requirement as these laws are silent on whether the data can be accessed and processed.

With regard to **the type of mandate**, the mandates vary from compelled storage of a mirror copy (Russia); to local storage (Indonesia), which means that data must be stored in servers physically located in that country; to local processing (Turkey, Nigeria, Venezuela for payments data), which means that any analysis or interpretation of that data must be carried out within that territory. Some Latin American countries restrict transfers of data outside the country if the recipient country does not have an adequate data protection framework, and other safeguards for protecting that data in place.

Countries that have **sector-specific restrictions** usually cover sensitive personal data (such as health records in Australia), crucial financial data (tax records in New Zealand) or data considered important for accountability and transparency in governance (Canada). The United States requires that all cloud computing services working for the Department of Defense (DoD) store data in U.S. territory.

Most of the instruments used to impose these restrictions were legislation - either wide-ranging or sector-specific. However, some countries impose these restrictions through guidelines (Nigeria) or regulations (Argentina).

[175] A. Segal, "Year in review: Chinese cyber sovereignty in action" 2017, <https://www.cfr.org/blog/year-review-chinese-cyber-sovereignty-action>

TABLE 2:DATA LOCALISATION AROUND THE WORLD[176]

#	COUNTRY	STRENGTH OF MANDATE	TYPE OF MANDATE	TYPES OF DATA TO WHICH MANDATE EXTENDS	SECTORS	LAWS IN QUESTION
1	**China**	Unconditional	Production (Local requirement), Local Storage, Local processing	Effectively all data-Critical Information Infrastructure, 'Important' personal information of any natural person collected or produced by Critical Information Infrastructure Operators (CIIO)	Cross-sector	China Cybersecurity Law, 2016; Trial Guidelines

[176] The following sources were used for constructing the table: ITI, Data Localisation Snapshot, July 29 2016,
<https://www.itic.org/public-policy/SnapshotofDataLocalizationMeasures7-29-2016.pdf>;
Data Protection Laws Of The World <https://www.dlapiperdataprotection.com/>;
N, Sen, Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?, Journal of International Economic Law, Volume 21, Issue 2, 1 June 2018, Pages 323–348
<https://academic.oup.com/jiel/article-abstract/21/2/323/5004397?redirectedFrom=PDF>

				including public communication and information services, Transport, energy, Water, finance, public services and governance		
2	**Indonesia**	Unconditional	Local Storage	Related to provision of 'public services	Cross-sector	Electronic Systems and Transactions ("GR 82")
3	**Nigeria**	Unconditional	Local processing (point-of-sale to ATM),Local storage (government ministries, departments, agencies)	Business, Personal, Government, Critical Information Infrastructure	Cross-sector	Guidelines for Nigerian Content Development in Information and Communications Technology (the NITDA Guidelines,2013 the National

						Information Systems and Network Security Standards and Guidelines
4	**Russia**	Unconditional	Local storage (mirroring), retention for twelve hours of all data on their servers	Personal data of Russian citizens	Cross-Sector	Law No. 242-FZ "On Amendments to Certain Laws of the Russian Federation in Order to Clarify the Procedure for Personal Data Processing in Information and Telecommunications Networks"
5	**Vietnam**	Unconditional	Local storage	All forms of personal	Cross-cutting	Vietnam Law on

				data belonging to Vietnamese citizens		Cybersecurity, 2018 (to come into effect Jan 2019)
6	**Kazakhstan**	Unconditional	Local storage	All 'databases' broadly defined as covering virtually any storage facility	Cross-cutting	Law No. 94-V on Personal Data and Protection of 21 May 2013 (the 'Personal Data Law'
7	**Australia**	Unconditional (sectoral)	Local storage, processing	Sensitive Personal	Health	Personally Controlled Electronic Health Records Act, 2012
8	**Canada**	Unconditional (sectoral)	Local storage and access	Data held by public bodies	Government	
9	**New Zealand**	Unconditional (sectoral)	Local storage	Business, Company (Tax Records)	Finance	Internal Revenue Act
10	**Taiwan**	Conditional, Sectoral	Government can restrict transfers on	Data for industries they regulate	Government	Taiwan Data Protection Act

			grounds of national security			
11	**Turkey**	Unconditional (sectoral)	Local processing	Payments Data	Financial	Payment and Security Reconciliation Systems, Payment Services, and Electronic Money Institutions,
12	**Venezuela**	Unconditional (sectoral)	Local processing	Payments data	Financial	
13	**South Korea**	Conditional for some sectors, Unconditional in other specified sectors	Restricted access (maps data), Local storage (certain financial companies and medical records)	Personal, sensitive, financial	Government, Financia, Medical	Korean Land Survey Act (South Korean maps data); Personal Information Protection Act;Supervision of Electronic Financial Transactions,

						Enforcement Rule of the Medical Service Act and the Standards of Facilities and Equipment for Management and Retention of Electronic Medical Records ("EMRs")
14	**Argentina**	Conditional Data can be transferred only if it will be protected in the target country and the country has an 'adequate' data protection	Conditional storage	All data	Cross-cutting	Regulation No. 60-E/2016

		framework, although numerous exceptions apply (including consent, contractual clauses, and binding corporate rules).				
15	**Colombia**	Conditional Transfers to countries that do not provide an adequate level of protection forbidden unless (i)express consent, (ii) for the purpose of preserving data subject's health	Conditional storage	All data	Cross-cutting	Law 1581

		and life, (iii)Banking or stock exchange transfers, (iv) In pursuance to international transfers, (v)For contractual purposes, (vi) Required to safeguard public interest				
16	**Uruguay**	Conditional transfers permitted to countries that do not provide adequate levels of protection y;transfer of company data only	Conditional storage	All data	Cross-cutting	Data Protection Act Law No. 18.331 (11 August 2008); Decree No. 414/009

		permissible when recipient company has adopted a code of conduct registered with the Unidad Reguladora Y De Control De Datos Personales (URDCDP)				
17	**United States of America**	Unconditional	Storage	"Critical information" that concerns "operational security,'	Defense/National Security	DoD interim Rule on Network Penetration Reporting and Contracting for Cloud Services
18	**European Union**	Conditional Transfers permitted only to countries	Conditional Storage	All personal data	Cross-cutting	The General Data Protection Regulation (EU)

		with an 'adequate' level of data protection; or through intra-company codes, or model contractual clauses approved by the European Commission. Transfers also permitted with explicit consent from the data subject, or in instances of necessity.				2016/679

Conclusions and Recommended Approaches

Our research suggests that the various proposed data localization measures, serve the primary objective of ensuring sovereign control over Indian data. Various stakeholders have argued that data localisation is a way of asserting Indian sovereignty over citizens' data and that the data generated by Indian individuals must be owned by Indian corporations.[177] It has been argued that Indian citizens' data must be governed my Indian laws, security standards and protocols.[178]

However, given the complexity of technology, the interconnectedness of global data flows, and the potential economic and political implications of localization requirements - approaches to data sovereignty and localization should be nuanced. In this section we seek to posit the building blocks which can propel research around these crucial issues. We have organized these questions into the broader headings of prerequisites, considerations, and approaches:

PRE-REQUISITES

From our research, we find that any thinking on data localisation requirements must be preceded with the following prerequisites, in order to protect fundamental rights, and promote innovation.

- **Is the national, legal infrastructure and security safeguards adequate to support localization requirements?**
  A number of infrastructural, financial and logistical requirements are key to supporting the local storage of data through the building of data centres. The e-commerce task force also recognizes these requirements and asks that these measures be implemented before a data localisation mandate is brought in.[179] These include[180]:
    - ★ Sustainability of energy consumption and the cost of other basic utilities

[177] See Annexure
[178] L Kathragadda and A Sengupta, "A Digital Dandi March:Push data localisation to preserve sovereignty and enable fair competition", 2018, <https://timesofindia.indiatimes.com/blogs/toi-edit-page/a-digital-dandi-march-push-data-localisation-to-preserve-indias-sovereignty-and-enable-fair-competition/>
[179] e-Commerce Task Force, Electronic commerce in india: Draft national policy framework (non-official version), Medianama, 2018, <https://www.medianama.com/wp-content/uploads/Draft-National-E-commercePolicy.pdf>
[180] V Choi, S. Huang, & M Law, State of cloud adoption in asia pacific, Cushman & Wakefield, 2016, <https://downloads.cloudsecurityalliance>

- ★ Wireless Bandwidth
- ★ Favourable tax regime that enables growth of data centres
- ★ Downstream infrastructure such as uninterrupted power supplies
- ★ Significant expenditure on cooling due to unfavourable weather patterns. An adequate costing of this is required to understand the impact of weather patterns on setting up of data centres.
- ★ Robust security safeguards which would include both **physical and logistical protection** for the data centres (including but not limited to access filters such as biometric authentication, for data centres containing sensitive personal information-armed personnel from law enforcement authority or a recognized private security company and strong physical fortifications), rigorous checks on the infrastructure to ensure it complies with infrastructural requirements to guarantee maximum safety and security and **technical measures** including but not limited to protection against unauthorized remote access to the data centre, maintenance of a back-up in another physical location.
- ★ The relevance of the dataset and the ability to accurately label and process them is crucial for curating a training dataset for an algorithm. Before devising policy measures that improve access to increased quantities of data, debunking India's capacity to process them is an imperative.

- **Is India's articulation of its broader vision for the future of the internet clearly articulated to prevent the breeding of incorrect perceptions among external stakeholders?** A clearly articulated strategy that outlines India's position in the global debate on cyber norms and its belief in the freedom of information across the internet. Despite being the world's largest democracy, India has been accused of 'digital authoritarianism' by actors in the West[181], which has caused some commentators to consider whether India is swinging towards democracy or authoritarianism.[182]

  The data localisation debate is not directly connected to these allegations. However, the absence of a clearly articulated strategy, could lead external actors,such as China to hope that the restrictions placed by India might be a

[181] Goel,Vindul (2019)," India proposes Chinese style internet censorship" Retreived from <https://www.nytimes.com/2019/02/14/technology/india-internet-censorship.html>
[182] Sherman, Justin (2019)," India's Digital Path:Leading Democratic or Authoritarian" Retreived from <https://www.justsecurity.org/62464/indias-digital-path-leaning-democratic-authoritarian/>

first step towards them adopting the Shanghai Corporation Organisation's 'information sovereignty' approach in the norms debate. This approach advocates for a tightly regulated internet with each sovereign government deciding the extent of civil liberties online.Given India's rich democratic tradition, the government should clearly state how they are placed in the debate over the future over the internet to in order to ensure that the pursuit of legitimate foreign policy goals such as cross border access to data are not misinterpreted as India swinging towards 'digital authoritarianism.'

- **Are human rights, including privacy and freedom of expression online and offline, adequately protected and upheld in practice?**
  Adequate protection for the rights of online users in India should be interpreted as a crucial aspect of data sovereignty. A comprehensive data protection legislation mandating high standards of privacy, and strong constitutional safeguards for freedom of speech and expression are therefore crucial prerequisites. The constitutional guarantee for freedom of expression guaranteed under Article 19 and the recognition of privacy as a fundamental right via the *Puttuswamy* judgment signals that we have a robust constitutional edifice which needs to be adapted to the digital sphere. A robust data protection and privacy framework can also enable innovation and support the local IT industry and data centers through better cross-border data flows.
- **Do domestic surveillance regimes have adequate safeguards and checks and balances?**
  The legal due process for lawful interception and surveillance needs significant reform in India to protect civil liberties of its citizens. For example, the government committee that must review requests under Section 69 of the IT Act meets at least once in two months.[183] However, an application under the Right to Information Act to the Ministry of Home Affairs in 2013 has revealed that on an average, upwards of 7500 to 9000 orders for interception are issued every month by the Central Government alone.[184] Therefore, if the review Committee meets once every two months as it is statutorily mandated to do,

[183] Rule 22, The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009
[184] India Today Web Desk, "RTI reveals UPA govt snooped on 9000 phone, 500 emails every month", 2018
<https://www.indiatoday.in/india/story/rti-reveals-upa-govt-snooped-on-9000-phones-500-emails-every-month-1415401-2018-12-22>

then it would have to consider and dispose of between 15000 to 18000 orders of interception at every meeting.

While protection from foreign surveillance is a noble objective, in the absence of adequate legal safeguards in Indian law, citizens may continue to be the subjects of constant scrutiny from the state.

- **Does the private and public sector adhere to robust privacy and security standards and what should be the measure to ensure protection of data?** Privacy and security also depends on organizational practice and policy-makers should actively consult individuals with operational experience, security researchers and lawyers in a multi-disciplinary effort. This can be defined by local law and industry best practice but it is important that the implementation of such law or best practice is audited and verified. All body corporates in India currently must implement ISO 27001 or similar industry standards as per section 43A of the IT act and associated rules. As a note, these provisions do not extend to the public sector. Furthermore, it is unclear the extent to which private companies are adhering and upholding the standard.

CONSIDERATIONS

- **What are the objectives of localization?**
    - **c. Innovation and Local ecosystem**
        i. The Srikrishna Committee Report specifically refers to the value in developing an indigenous Artificial Intelligence ecosystem. Much like the other AI strategies produced by the NITI Aayog and the Task Force set up by the Commerce Department, it states that AI can be a key driver in all areas of economic growth, and cites developments in China and the USA as instances of reference. The Report also cites a paper authored by Azmeh and Foster which highlights benefits of a data localization policy for developing countries. [185] These benefits include (1) increased foreign direct investment in digital infrastructure and (2) positive spill-over effects of an indigenous market for data centres through enhanced connection, job creation and the presence of

[185] S. Azmeh, and C.G. Foster, The TPP and the digital trade agenda: Digital industrial policy and Silicon Valley's influence on new trade agreements. Working Paper. International Development, Working Paper Series (16-175). Department of International Development, 2016 <http://eprints.whiterose.ac.uk/125522/>.

skilled professionals. As envisioned in the draft e-commerce policy, if data is stored in India it can be shared with start-ups towards enabling innovation and can be made available to users for portability if so desired.

d. National Security, Law Enforcement and Protection from Foreign Surveillance

i. Access to data by domestic law enforcement authorities is an important aspect of sovereign control over data. As recognised by the Srikrishna White Paper, a disproportionate amount of data belonging to Indian citizens is stored in the United States and the presently existing Mutual Legal Assistance Treaties process (MLATs) through which Indian law enforcement authorities gain access to data stored in the US is excessively slow and cumbersome.

ii. The Srikrishna Committee Report argues that restricting the storing and processing of data within Indian territory may protect against foreign surveillance from agencies largely headquartered in the US.

iii. The Srikrishna Committee report also cites studies which suggest that undersea cable networks that transmit data from one country to another are vulnerable to attack. Therefore, it argues that processing critical data on Indian territory would minimise the vulnerability of relying on undersea cables. It cites a report by Policy Exchange that states that the threat to undersea cables by Russian actors may be an existential one for the UK.

- **What are the potential spill-overs and risks of a localisation mandate?**

Diplomatic and political: Despite the WTO not having any precedent against restrictions on cross-border data transfers, our research showed multiple ways in which any localisation gambit may open India up to litigation at the WTO for violations of the provisions of the GATS. In the shorter term, however, it may act as a thorn in configuring trade relationships with groups like the EU and the USA. It is crucial to note that a trade agreement is a multivariate relationship, and restrictions on the flow of data often might lead negotiating parties to impose tariffs in other spheres. The prospect of data localization has already come up as an issue in the Indo-US trade relationships as negotiators got into talks to review India's eligibility under the Generalised System of

Preferences (GSP) that allows India to export around 2,000 product lines under 'zero tariffs.'[186] On March 4, 2019, US President Donald Trump revoked India's developing country status under the GSP.

Security risks (" Regulatory stretching of the attack surface"): Storing data in multiple physical centres naturally increases the physical exposure to exploitation by individuals physically obtaining data or accessing the data remotely. So, the infrastructure needs to be backed up with robust security safeguards and significant costs to that effect.

Economic impact: Restrictions on cross-border data flow may harm overall economic growth by increasing compliance costs and entry barriers for foreign service providers and thereby reducing investment or passing on these costs to the consumers. The major compliance issue is the significant cost of setting up a data centre in India combined with the unsuitability of weather conditions. Further, for start-ups looking to attain global stature, reciprocal restrictions slapped by other countries may prevent access to the data in several other jurisdictions.

What are the existing alternatives to attain the same objectives?
The Indian government has sought to meet a diverse set of policy objectives through its proposed localization mandates. It must also be evaluated whether these objectives may be better fulfilled using alternatives specifically addressed to them. For instance, tax avoidance by online entities that generate significant revenue from India suggests a lacuna in India's taxation framework, and not a flaw in data storage practices. Amending the Finance Act (for instance, by incorporating the Significant Economic Presence standard) could thus be a more effective remedy than mandatory localization. While the feasibility of all these alternatives needs to be questioned and piloted, they may be more suitable to achieve the desired objectives, while avoiding the negative consequences of localisation.

In a similar vein, our research suggests that data localization alone cannot fully achieve national control of data at rest and in motion. For instance, the challenges faced by law enforcement agencies in obtaining data may be more accurately characterized as an outcome of the absence of international

[186] Hindu Editorial, "No zero-sum games: On India-US trade hostilities", 2019, <https://www.thehindu.com/opinion/editorial/no-zero-sum-games/article26231336.ece>

consensus on cross-border access to data. Many countries have developed legislation with extra-territorial mandates over data, which would continue to be applicable even if data is stored within India. Localization would not address the conflict of law issues that may inhibit foreign entities from sharing data with Indian law enforcement. Instead, relying on the principles of International Law and developing a robust privacy-centric domestic regime in order to bolster India's position in these negotiations should be the first order of priority.

The objective and potential alternatives are listed below:

OBJECTIVE	**ALTERNATE**
Law enforcement access to data	Access to data is a concern for all countries where data is not typically hosted by global corporations. Pursuing international consensus can therefore be a beneficial strategy. India must improve its position with respect to instruments such as the CLOUD Act, and the EU's e-Evidence Directive. Irrespective of the location of data, Indian law enforcement requests would have to comply with such instruments, if applicable. This also entails introducing a stronger data protection framework, since such instruments often require the presence of appropriate safeguards for personal data.
Widening tax base by taxing entities that do not have an economic presence in India	Equalisation levy/Taxing entities with a Significant Economic Presence in India, although India would still need to develop an adequate mechanism for enforcement of the tax claims under such measures.

Threat to fibre-optic cables	Building of strong defense alliances with partners to protect key choke points from adversaries
Boost to US based advertisement revenue driven companies like Facebook and Google ('data colonisation')	Developing robust standards and paradigms of enforcement for competition law such as Germany's recent ruling from the Federal Cartel Office which stated that bars Facebook from, in effect, forcing users to agree to unrestricted collection and assigning of non-Facebook data to their Facebook accounts.[187]

APPROACH

- **What data might be beneficial to store locally for ensuring national interest? be mandated to stay within the borders of the country? What are the various models that can be adopted?**

a. **Mandatory Sectoral Localisation:** Instead of imposing a generalized mandate, it may be more useful to first identify sectors or categories of data that may benefit most from local storage. For instance, Australia localizes personal data related to health, on account of its highly sensitive nature. The United States mandates localisation of defense sector data due to national security reasons. Category specific mandates can also be tailored according to the nature and type of data. For instance, the Personal Data Protection Bill, 2018 imposes a complete bar on cross border transfers of data that is deemed 'critical.' This is a stronger restriction than that imposed on other types of personal data - which is allowed to be mirrored in territories outside of India.

*National Security***:** While the NCIIPC lists 5 sectors as critical, (i) power and energy; (ii) banking, financial services and insurance ("BSFI"); (iii)

[187] Dreyfuss E, "German Regulators just outlawed Facebook's whole ad business", 2019, <https://www.wired.com/story/germany-facebook-antitrust-ruling/>

ICTs; (iv) transportation and (v) e-governance and strategic public enterprises, these categories are insufficiently precise. For instance, the benefits from localizating all data related to ICTs or transportation are not evident. Instead, within these sectors, specific types of data such as those related to payments data or defense would need to be identified and accordingly localisation may be mandated.

Sensitive Personal Information which includes passwords, financial data, health data, official identifier, sexual orientation, biometric data, genetic data, caste or tribe. The theoretical reason for mandating localization of sensitive personal information could be that the sovereign, which is answerable to its citizens, has a higher duty to protect such data in its territory.

b. 'Conditional ('Soft') Localisation: For all data not covered within the localisation mandate, India should look to develop conditional pre-requisites for transfer of all kinds of data to any jurisdiction, like the Latin American countries, or the EU. This could be conditional on two key factors:

Equivalent privacy and security safeguards: Transfers should only be allowed to countries which uphold the same standards. In order for this, India must also develop and incorporate robust privacy and security protections. This would not only ensure that all Indian citizen's data are protected by uniform security standards, but also play a positive role in bolstering India's global image as a nation committed to upholding human rights norms both within and outside the country.

Agreement to share data with law enforcement officials when needed: Given the large number of requests from foreign politicians, business guilds and corporations to retract localisation mandates, India could use the proposed localisation mandate in the draft of the Sri Krishna Bill to improve its position in diplomatic negotiations. Now that the threat of potential localisation exists, India should use the threat to put pressure on countries like the US,where a lion's share of data is stored, to develop mechanisms that solve the fetters that exist in present data sharing agreements.Instead of mandatory localisation, we should make transfer of data to any jurisdiction contingent on a bilateral agreement that enables instantaneous sharing of data based on Indian laws with Indian authorities. Further, the agreement must also ensure that under

no condition should the business entity make the data available to a foreign government even if the consumer consents.

By placing these conditions, India would be asserting data sovereignty without engaging in unwarranted nationalism that could potentially harm both India's economy and India's standing on the world stage in the long run.

Annexure I

Mapping Data Localization Requirements Across Different Jurisdictions

Canada

In Canada, the provinces of British Columbia and Nova Scotia have adopted laws that require public bodies to store and access their data domestically and requires third parties providing services under a government contract to do the same. In British Columbia these requirements were enacted in response to concerns that the US government could access the personal data of citizens under the Patriot Act and require public bodies to ensure personal information as defined by the Act is stored and accessed only in Canada. Demonstrating the complexity of implementing data localization requirements, the Act provides for two exceptions to this rule 1. If consented to by the individual 2. If allowed for under FOIPPA i.e when required or authorized by other laws in Canada or British Columbia, if required by a treaty or agreement, to government for specified uses, for the purpose of licensing, registration, insurance, investigation or discipline of persons, if compelling circumstances exist that affect anyone's health or safety, to a law enforcement agency under an agreement or treaty. Temporary access and storage is permitted for installing, implementing, maintating, repairing etc. electronic systems, for data recovery being undertaken following failure of an electronic system, and when employees or service providers are traveling temporarily outside of Canada.[188] Nova Scotia enacted similar provisions under the Personal Information International Disclosure Protection Act. The Act applies to service providers or associates of service providers. The Act contains similar (with some differences) exceptions as FOIPPA and includes storage and access with authorization by the head of a public body if it meets requirements for the public body's operation.[189] In a much softer approach, Quebec amended the Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information to require that before releasing information under the Act outside of Quebec, public bodies must ensure that it receives equivalent protections. Alberta has taken a different approach by mirroring the provisions in the federal Privacy Act but with the change that courts must have jurisdiction in Alberta. In practice this means that a public body or its service

[188] F Cate, "Provincial Canadian Geographic Restrictions of Personal Data in the Public Sector", 2008, <https://www.huntonak.com/files/Publication/2a6f5831-07b6-4300-af8d-ae30386993c1/Presentation/PublicationAttachment/0480e5b9-9309-4049-9f25-4742cc9f6dce/cate_patriotact_white_paper.pdf>
[189] Ibid.

provider would be violating the law if it provides data to a subpoena, warrant, or order issued in another province or country.[190]

Brazil

In response to the Snowden revelations, then Brazilian President proposed an amendment to Brazil's draft internet regulatory model (Marco Civil a Internet) that included provisions which would have introduced penalties for breach of upto 10 percent of the previous year's revenue.

Sectors in Brazil have seen proposals for data localisation requirements. For example, in 2017 the Central Bank of Brazil proposed a draft resolution (57/2017) which contains a requirement for local data storage of financial data.[191] An earlier draft of the Marco Civil da Internet, Brazil's 'Internet Bill of Rights', included a clause mandating data localization.[192] The requirement was introduced as a response to the Snowden revelations. However, on account of opposition from various fronts,[193] the requirement was removed, and replaced with a clause asserting Brazilian jurisdiction over data and services offered in Brazil.[194]

Russia

The Russian Federal Law No. 242-FZ, an amendment to previous Federal Law, mandates that companies collecting personal information about Russian citizens must "record, systematize, accumulate, store, clarify (update or modify) and retrieve" the information using servers physically located within Russia.[195] Operators must also notify the regulator about the physical locations of their databases, when commencing data processing operations. The Law became effective from September

[190] Ibid.
[191] ITIF, "Response to Central Bank of Brazil Comments on Cybersecurity Policy", 2017, <http://www2.itif.org/2017-brazil-central-bank-data-localization-english.pdf>
[192] Ibid
[193] B. Douglas, Brazil's Plan to Isolate Its Internet Is a Terrible Idea., 2013 <https://motherboard.vice.com/en_us/article/kbzeje/why-brazils-new-internet-law-is-stup>; M. Angelica, "Companies brace for Brazil local data storage requirements", 2014 <https://www.zdnet.com/article/companies-brace-for-brazil-local-data-storage-requirements/>
[194] C. A. Souza, F. Steibel & R. Lemos, Notes on the creation and impacts of Brazil's Internet Bill of Rights, The Theory and Practice of Legislation, 2017, <https://itsrio.org/wp-content/uploads/2017/01/Notes-on-the-creation-and-impacts-of-Brazil-s-Internet-Bill-of-Rights.pdf>
[195] Article 1(2), Article 2(1), Federal Law No. 242-FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks (with Amendments and Additions) <https://pd.rkn.gov.ru/authority/p146/p191/>

2015, and also empowers the regulator (the Roskomnadzor) to block access to websites that are found to be in violation of the law.[196]

The Russian Ministry of Communications issued a non binding guidance in August 2015, in order to clarify the scope of the law.[197] The Ministry noted that the Law applies to all operators (online or offline) within the Russian Federation, as well as websites whose business activities are oriented towards a Russian audience. However, the mere fact of the website being accessible from Russia would not be sufficient. Relevant criteria could be, the use of localized top level domain names, the availability of Russian language versions of the website, the presence of Russian language ads, and the ability to transact in Rubles.[198] Further, the data collection must be purposeful, and not incidental. Instances where data is received by an entity from another entity in the context of routine business activities would also be exempt.[199] However, the Law would apply if automated processing is employed to collect personal data from third parties.[200] Another crucial clarification is that the Law does not prohibit the transfer of data outside Russia. Thus, personal data may be first stored in a primary database within Russia, and can be transferred to servers abroad, subject to the relevant restrictions on cross border transfers. Any changes to the data must first be made in the database located within Russia, and then reflected on any server abroad.[201]

[196] Ibid.
[197] Processing and storage of personal data in the Russian Federation. Changes from September 1, 2015, February 12 2016, <https://minsvyaz.ru/ru/personaldata/#1438546984884>; S. Blagov, Russia Clarifies Looming Data Localization Law, August 10 2015, <https://www.bna.com/russia-clarifies-looming-n17179934521/>; Borenius Legal Alerts, Official clarifications regarding the data localization requirement, 2015 <https://www.borenius.ru/en/2015/08/07/official-clarifications-regarding-the-data-localization-requirement/>;
N. Gulyaeva, M. Sedykh and B. Cohen, Russia Update: Regulator Publishes Data Localization Clarifications, August 11 2015, <https://www.hldataprotection.com/2015/08/articles/international-eu-privacy/russia-update-regulator-publishes-data-localization-clarifications/>
[198] Ibid.
[199] Ibid.
[200] Ibid.
[201] Ibid.

It is reported that the Roskomnadzor routinely conducts audits and inspections,[202] along with releasing data about the results of such enforcement procedures.[203] In 2016, the Moscow City Court affirmed an request by the Roskomnadzor to block LinkedIn for continuing to violate the data localization law.[204] Russian authorities also directed Google and Apple to remove LinkedIn from the Russian version of their App Stores.[205] In 2018, Roskomnadozor officials stated that Facebook and Twitter would soon be made to comply as well.[206]

European Union

In the European Union, personal data flows are governed by the General Data Protection Regulation (2016/679), which replaced the EU's Data Protection Directive (95/46/EC) in 2018. According to Article 45 of the GDPR, personal data may only be transferred to a country, organization of territory that provides an 'adequate level of protection'.[207] The European Commission must make such assessments regarding the level of protection, taking into account factors such as the rule of law, respect for human rights, independent supervisory authorities, etc. The adequacy decisions may also be limited to specific territories, or specific sectors within a country. The EC must also periodically review and monitor such assessments.

In the absence of an adequacy decision, personal data can be transferred outside the EU only if the controller or processor provides appropriate safeguards, and if enforceable data subject rights with effective legal remedies are available to data subjects.[208] Article 46 lists the various mechanisms that may be available, including

[202] N. Gulyaeva, M. Sedykh and B. Cohen, Russia Releases Data Localization Inspection Plan for 2016, February 4 2016, <https://www.hldataprotection.com/2016/02/articles/international-eu-privacy/russia-releases-data-localization-inspection-plan-for-2016/>

[203] N. Gulyaeva, M. Sedykh and B. Cohen, Russia Data Localization Update: Results from Regulatory Inspections Clarify Enforcement Approach, June 23, 2016, <https://www.hldataprotection.com/2016/06/articles/international-eu-privacy/russia-data-localization-update-results-from-regulatory-inspections-clarify-enforcement-approach/>.

[204] M Maalouf, K Lamont, Russia Steps Up Enforcement Of Data-Localization Law, November 16, 2016, <https://blog.zwillgen.com/2016/11/16/russia-blacklists-linkedin-over-data-localization-law/>

[205] C. King, K. Benner, Russia Requires Apple and Google to Remove LinkedIn From Local App Stores, January 6 2017, <https://www.nytimes.com/2017/01/06/technology/linkedin-blocked-in-russia.html>

[206] Sputnik News, Russian Watchdog to Ask Twitter, Facebook for Personal Data Localization in Dec., September 18, 2018, <https://sputniknews.com/russia/201809181068127798-russia-twitter-roskomnadzor-letter/>
Interfax Ukraine, Roskomnadzor: Facebook to stop working in Russia in 2018 unless complies with personal data localization law, September 26, 2017, <https://www.kyivpost.com/russia/roskomnadzor-facebook-stop-working-russia-2018-unless-complies-personal-data-localization-law.html>

[207] Article 45 GDPR

[208] Article 46 GDPR

approved intra-company codes, and model contractual clauses adopted by the EC.[209] Further, Article 49 allows derogations that permit transfers in the absence of an adequacy decision or appropriate safeguards.[210] These include grounds such as necessity, and the explicit, informed consent of the data subject.

The European Union does not mandate the retention of data within its territory as such. However, it has been argued that imposing a complex set of conditions that must be complied with for cross border transfers of data acts, in effect, as a mandate for localization.[211] Controllers may find it easier and cheaper to store data within the European Union rather than navigate the complex requirements imposed by the EU, or risk falling short of compliance. However, it is important to note that data may be freely stored outside the EU as long as the jurisdiction has received an adequacy status.

In November 2018, the European Parliament and Council passed the Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union.[212] The Regulation prohibits data localization by Member States for all data that is not covered by the GDPR. Local storage may be mandated only on the grounds of public security, and any data localization mandates must be communicated to the European Commission, in order to ensure compliance.

China

China has devised and implemented a broad data localization law. The Standing Committee of the National People's Congress of China passed a Cybersecurity Law on 7 November, 2016.[213] Article 37 of China's Cybersecurity Law requires "critical information infrastructure" operators to store within mainland China all personal information and important data gathered or produced within the mainland territory, which the definition of "critical information infrastructure" is introduced in Article 31 to include but is not limited to "public communication and information services,

[209] Article 46 GDPR
[210] Article 49 GDPR
[211] Chander and Le Anupam Chander, Uyên P. Lê, Data Nationalism, 64 Emory L.J. 677 (2015), <http://law.emory.edu/elj/content/volume-64/issue-3/articles/data-nationalism.html>
[212] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1546942605408&uri=CELEX:32018R1807>
[213] Y. Wei, Chinese Data Localization Law: Comprehensive but Ambiguous, February 7 2018, <https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/>

energy, transportation, water resources, finance, public services, e-governance".[214] China's cybersecurity law which took effect in June 2017 requires all firms operating in China to store data collected in China on servers located in Chinese territory. In addition, any one who publishes online content must ensure that " necessary technical equipment, related servers and storage devices" are located in China. Firms and individuals that are data processors are obliged to store all data in China and online maps must also be stored on a server in China. [215]Further, a significant portion of data cannot even be transferred out without a security assessment conducted by a government official. Foreign firms cannot provide cloud computing services if a Chinese partner does not own at least 50% of the joint venture (JV)

Therefore, Apple has began hosting the iCloud accounts in China in partnership with state-owned Guizhou-Cloud Big Data Industry Co. Ltd. Another draft encryption law passed in April 2017, Apple also stores its cryptographic keys that unlock the iCloud accounts in Chinese data centres-as opposed to in the USA, which was the case till now. [216]

Annexure 2

A survey of stakeholder responses

No.	Organisation	Nature of Organisation	Stance	Points of Concern/Support On Data Localization	Recommendations /Suggestions
1	Access Now[217]	Non-Profit (Research & Advocacy)	Against	Dilutes India's connection to the global internet. Open to third party abuse. High	None Given

[214] Y. Wei, Chinese Data Localization Law: Comprehensive but Ambiguous, February 7 2018, <https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/>
[215] HFW, China: Cybersecurity Law and Data Localisation, October 16 2018, <https://www.lexology.com/library/detail.aspx?g=ee05d71c-fe7f-44ca-87ce-6ae0afb74071>
[216] S. Liao, Apple officially moves its Chinese iCloud operations and encryption keys to China, February 28 2018, <https://www.theverge.com/2018/2/28/17055088/apple-chinese-icloud-accounts-government-privacy-speed>

				cost of compliance.	
2	National Institute of Public Finance Policy - Bailey, Parsheera Bhandari and Rahman[218]	Think-tank	Against	Localisation only in cases where the benefits outweigh costs.	Reconsider mirroring of critical personal data. Requires cost-benefit analysis and public consultation.
3	Ikigai Law[219]	Law Firm	Against	No suitable domestic service provider. Effects startup and health sector.	Calls for reassessing these provisions and addressing stakeholder concerns.
4	BankBazaar[220]	Private Company	Against	Lead to restructuring of global systems - impact performance and companies exiting the market.	Removal of mandatory localisation - high costs to comply. Hamper digital economy.
5	Broadband India Forum[221]	Think-tank	Against *Mandatory* Data	Effect consumer interests and medical research.	MSMEs may choose domestic or foreign

[217] Access Now, Assessing India's Proposed Data Protection Framework: What The Srikrishna Committee Could Learn From Europe's Experience, September 2018, <https://www.accessnow.org/cms/assets/uploads/2018/09/Assessing-India%E2%80%99s-proposed-data-protection-framework-final.pdf>

[218] R Bailey, V Bhandari and ors, Response to the Draft Personal Data Protection Bill, 2018, October 20 2018, <https://blog.theleapjournal.org/2018/10/response-to-draft-personal-data.html>

[219] Ikigai Law, Comments of certain start-ups on the Personal Data Protection Bill, 2018: Consolidated views, October 17, 2018, <https://www.ikigailaw.com/comments-of-certain-start-ups-on-the-draft-personal-data-protection-bill-2018-consolidated-views/#acceptLicense>

[220] A&A Dukaan Financial Services Private Limited (Bankbazaar.Com), Suggestions On Draft Personal Data Protection Bill, September 27 2018, <https://www.medianama.com/wp-content/uploads/BankBazaar-Submission-India-Draft-Data-Protection-Bill-Privacy-2018.pdf>

			Localisation	Enhance security with better technical measures.	providers. Only mandatory for select industries. Strengthen bilateral/multilateral ties.
6	CCAOI[222]	Non-Profit (Research)	Against	Serving copy of personal data not solution to data security.	Make laws to enable access by law enforcement with adequate oversight.
7	CUTS International [223]	Think-tank	Against	Cost of services increases for consumers. Effect SMEs	A more evidence-based approach rather than assumptions would be beneficial in formulating policies.
8	CSRC & CPF[224]	Think-tank	Against	Serving copies still susceptible to attack. Against principles of data privacy.	None Given
9	Dvara Research[225]	Think-tank	Against	Scope of “necessity or strategic interests of the state”	Must provide sufficient substantive policy and principles to

[221] BIF Submission/Comments on Draft Personal Data Protection Bill 2018 <https://www.medianama.com/wp-content/uploads/Broadband-India-Forum-Submission-India-Draft-Data-Protection-Bill-Privacy-2018.pdf>
[222] CCAOI Submission on Draft Personal Data Protection Bill 2018 <https://www.medianama.com/wp-content/uploads/CCAOI-Submission-India-Draft-Data-Protection-Bill-Privacy-2018.pdf>
[223] CUTS Comments on Draft Personal Data Protection Bill 2018 <http://www.cuts-ccier.org/pdf/Advocacy-CUTS_Comments_on_the_draft_Personal_Data_Protection_Bill2018.pdf>
[224] Proceedings Of Workshop Conducted On Draft Data Protection Bill (2018), <https://www.medianama.com/wp-content/uploads/Cyber-Security-Research-Centre-Punjab-Engineering-College-Submission-India-Draft-Data-Protection-Bill-Privacy-.pdf>

				unclear. Differential protection for data - ineffective.	guide delegated legislation.
10	EC Directorate-General for Justice & Consumers[226]	Government/ International Organisation	Against	Create difficulties in conflict of law where contrary requirements exist. Hinder business and investment.	Supports free cross-border data flow and use of contractual instruments. Cites Budapest Convention.
11	Edge Networks [227]	Private Company	Against	Hinders innovation and ease of business for businesses especially SMEs.	None Given
12	Foundation of Data Protection Professionals in India[228]	Company	For	None Given	Personal data of foreigners/activities not related to India to be exempted.
13	Internet Democracy Project[229]	Non-Profit advocacy	Against (conditional)	Mirroring defeats justification for localisation. Unclear procedure on law enforcement access. Data	May be adopted for specific sectors like defense.

[225] CUTS Comments on Draft Personal Data Protection Bill 2018 <http://www.cuts-ccier.org/pdf/Advocacy-CUTS_Comments_on_the_draft_Personal_Data_Protection_Bill2018.pdf

[226] Submission on draft Personal Data Protection Bill of India 2018 by the Directorate-General for Justice & Consumers to the Ministry of Electronics and Information Technology (MeitY) <https://eeas.europa.eu/delegations/india/53963/submission-draft-personal-data-protection-bill-india-2018-directorate-general-justice_en>

[227] Edge Networks, Recommendations for Personal Data Protection Bill, <https://www.medianama.com/wp-content/uploads/Recommendations-for-Personal-Data-Protection-Bill_EdGE-Networks.pdf>

[228] Foundation of Data Protection Professionals in India, Comments on the Draft Personal Data Protection Bill, <http://fdppi.in/library/2018/fdppi_comments_pdpa2018_final.pdf>

				centres requires heavy power generation in India.	
14	Mozilla Foundation[230]	Non-Profit	Against	Need robust laws governing data controllers to protect privacy. Serious impact on Indian economy.	Using EU standards - eases global expansion and investment. Transfers via BCRs. Legal framework for surveillance with checks.
15	Information Technology Industry Council (ITI)[231]	Think-tank	Against	Makes data more vulnerable to attacks. Localisation is not a prerequisite for access or privacy.	Using alternative globally oriented mechanisms.
16	Khurana & Khurana[232]	Law Firm	Against	Definitions lack clarity. Mirroring raises privacy concerns and increases costs for data fiduciaries.	None Given
17	Mani Chengappa Mathur[233]	Law Firm	Unclear	None Stated	Requires clarification on the use of only one set of standard

[229] Internet Democracy Project, Is the fourth way going far enough? Our submission to MEITy on draft Personal Data Protection Bill 2018, <https://internetdemocracy.in/reports/pdpb/>
[230] Mozilla Submission on Draft Personal Data Protection Bill 2018 <https://blog.mozilla.org/netpolicy/2018/06/22/data-localization-india/>
[231] ITI Submission on Draft Personal Data Protection Bill 2018 <https://www.medianama.com/wp-content/uploads/ITI-Submission-India-Draft-Data-Protection-Bill-Privacy.pdf>
[232] Khurana and Khurana Submission on Draft Personal Data Protection Bill 2018 <http://www.khuranaandkhurana.com/2018/09/07/observationsrecommendations-on-personal-data-protection-bill-2018/>

					contractual clauses.
18	Observer Research Foundation[234]	Think-tank	Against	Difficulty in identifying nationalities of data owners. Hinders innovation and ease of business.	Should be the last resort. Harmonising regimes and a common framework is a better alternative.
19	Professor Graham Greenleaf[235]	Academic	Against	Statutory authorities lack independence. Approach too generic and regulations framed may be authoritarian.	None Given
20	US-India Strategic Partnership Forum (Visa, MasterCard, Amex, Amazon and Western Union)[236]	Non-Profit (Research & Advocacy)	Against	No evidence of corresponding benefits. "Serving copy" no definition. Economic impact of storing "critical personal data".	Deletion of "serving" under section 40. Storage should be case-specific or for national security.

[233] Mani Chengappa Mathur Submission on Draft Personal Data Protection Bill 2018 <https://www.medianama.com/wp-content/uploads/Mani-Chengappa-Mathur-Submission-India-Draft-Data-Protection-Bill-Privacy-2018.pdf>

[234] ORF Submission on Draft Personal Data Protection Bill 2018, <https://www.orfonline.org/wp-content/uploads/2018/10/ORF-PDPA-Submissions-.pdf>

[235] G. Greenleaf, GDPR-Lite and Requiring Strengthening – Submission on the Draft Personal Data Protection Bill to the Ministry of Electronics and Information Technology (India), September 20, 2018 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3252286>.

[236] USISPF Submission on Draft Personal Data Protection Bill 2018, <https://www.medianama.com/wp-content/uploads/USISPF-Submission-India-Draft-Data-Protection-Bill-Privacy-2018.pdf>

21	SFLC[237]	Non-Profit (Advocacy)	Against	Unviable in a globalised world. Prevents cross-jurisdictional checks on surveillance. Unclear on acceptable standard contractual clauses.	Data localization should not be a blanket requirement - limited to certain industries like health and finance. Must explore building bilateral data sharing agreements.
22	ZoomCar[238]	Company	Unclear	None Given	Clarifying the term "serving copy of personal data".
23	TechUK - Information Technology Telecommunications and Electronics Association[239]	Company	Against	Disrupts business operations and increases costs. Can compromise security of personal data.	Removal of provisions on localisation and storing of critical personal data. Use of international mechanisms instead.
24	Takshashila Institution[240]	Think-tank	Against	Hinders innovation and foreign investment. Potential for	Defining the term "critical personal data" and limiting the scope of localisation to

[237] SFLC Submission on Draft Personal Data Protection Bill 2018, <https://privacy.sflc.in/our-comments-draft-data-protection-bill/#recommendations>
[238] Zoomcar Submission on Draft Personal Data Protection Bill 2018, <https://www.medianama.com/wp-content/uploads/Zoomcar-Submission-India-Draft-Data-Protection-Bill-Privacy-2018.pdf>
[239] Tech UK Submission on Draft Personal Data Protection Bill 2018, <https://www.techuk.org/insights/reports/item/14021-techuk-position-paper-on-india-data-protection-bill?utm_source=contentstudio&utm_medium=referral>

				abuse. Definitions lack clarity.	critical personal data.
25	Facebook - Rob Sherman, Deputy Chief Privacy Officer [241]	Private Company	Against		Institute a certification process requiring digital companies to fulfil standards on data protection and privacy.
26	Mukesh Ambani - Chairman, RIL [242]	Company	For	Indian data should be owned by Indians and not global corporation. Data colonisation is detrimental.	
27	SAP[243]	Software Company	Against	Localisation will impact innovation	
28	Big Basket - Rakshit Daga, VP, Engineering[244]	E-commerce Company	For	Speeds up transactions and reduces network latency. BigBasket saw a 10% increase in efficiency.	

[240] Takshashila Submission on Draft Personal Data Protection Bill 2018, <https://takshashila.org.in/wp-content/uploads/2018/10/TPA-Comments-to-the-Draft-Personal-Data-Protection-Bill-2018-AP-MV-2018-02.pdf>
[241] M. Mandavi, Facebook executive bats for data certification of companies, December 19 2018, <https://economictimes.indiatimes.com/tech/internet/facebook-executive-bats-for-data-certification-of-companies/articleshow/67154479.cms>
[242] Mukesh Ambani says 'data colonisation' as bad as physical colonisation, December 19 2018, <https://economictimes.indiatimes.com/news/company/corporate-trends/mukesh-ambani-says-data-colonisation-as-bad-as-physical-colonisation/articleshow/67164810.cms>
[243] A. Pramanik, Data localisation push may impact innovation: SAP, December 3, 2018, <https://economictimes.indiatimes.com/tech/ites/data-localisation-push-may-impact-innovation-sap/articleshow/66926875.cms>
[244] S. Singh, D. Narayanan, India's data localisation push can give rise to new business opportunity, October 25 2018, <https://economictimes.indiatimes.com/tech/hardware/indias-data-localisation-push-can-give-rise-to-new-business-opportunity/articleshow/66356125.cms>

29	PwC - Siddharth Vishwanath, Partner, Cybersecurity [245]	Private Company (Advisory)	For	During war or hostilities, data centres could be switched off, local infrastructure is the solution.	
30	CtrlS Datacentres - B Srinivasa Rao, CMO[246]	Company runs Data centres	For	Localisation in India is a cost saver by about 80 per cent compared to a top-tier data centre.	
31	Alibaba - Simon Hu, President Alibaba Cloud [247]	Private Sector Tech Company (Foreign)	For	India needs to store its data in India. Has two data centres in India and looking to expand.	
32	John Cornyn, Mark Warner - US Senators[248]	Co-chairs, Senate, India caucus	Against	Acts as a "key-trade barrier" between India and the US.	Concerns regarding protection, security and access to data for lawful purposes could be addressed using alternatives.
33	Shamika Ravi, Research Director Brookings	Member of PM Economic Advisory Council	For	India's demands are part of a growing trend among other	

[245] Ibid.
[246] Ibid.
[247] M. Variyar, Alibaba backs data localisation in India, September 20, 2018, <https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/alibaba-backs-data-localisation-in-india/articleshow/65869841.cms>
[248] A. Kalra, Exclusive: U.S. senators urge India to soften data localization stance, October 13 2018, <https://www.reuters.com/article/us-india-data-localisation-exclusive/exclusive-u-s-senators-urge-india-to-soften-data-localization-stance-idUSKCN1MN0CN>

	India[249]			nations. Long-term strategic and economic interests.	
34	VFS Global[250]	International visa outsourcing & administration company	Against	Estimates a cost of 3 million euros to migrate the data excluding annual costs.	
35	Bhavin Turakhia, co-founder of Zeta and Flock [251]	Zeta - employee benefits company; Flock - messaging service for enterprises	For (Only Financial Data)	Supports storing of sensitive data like financial data locally while suggesting data mirroring in other cases.	
36	Sundar Pichai, CEO Google[252]	Private Sector (Foreign)	Against	Cross-border data flow encourages foreign investment and startups to expand globally.	
37	Paytm[253]	Private Sector (Indian)	For (Regarding RBI	Promote 'data sovereignty' over 'data	

[249] A. Kalra, A. Shah, Exclusive: U.S. tech giants plan to fight India's data localisation plans, August 20 2018, <https://in.reuters.com/article/india-data-localisation/exclusive-u-s-tech-giants-plan-to-fight-indias-data-localisation-plans-idINKCN1L506U>

[250] M. Mandavi, Moving data to India will cost 3 mn euros: VFS Global, November 19 2018, <https://economictimes.indiatimes.com/tech/internet/moving-data-to-india-will-cost-3-mn-euros-vfs-global/articleshow/66686742.cms>

[251] M. Variyar, Turakhia says ‘cliques’ pushing for localisation to thwart global companies, October 12, 2018, <https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/turakhia-says-cliques-pushing-for-localisation-to-thwart-global-companies/articleshow/66173253.cms>

[252] S. Agarwal, Sensitive data definition to be sector-specific, October 22 2018, <https://economictimes.indiatimes.com/news/economy/policy/sensitive-data-definition-to-be-sector-specific/articleshow/66309731.cms>

			Circular)	monopolisation'. Financial data should be considered 'critical personal data'	
38	PhonePe[254]	Private Sector (Indian)	For (Regarding RBI Circular)	Best for the long-term security of India's financial security services.	
39	Internet and Mobile Association of India (IAMAI)[255]	Private Sector (Indian)	Against	Restrictions on storage and collection of data hinders operation of startups.	
40	NASSCOM[256]	Private Sector (Indian)	Against	Cites hurdles for startups wishing to expand globally and rising costs for other companies.	
41	Mohandas Pai, CFO Infosys[257]	IT Company (Indian)	For (Regarding RBI Circular)	Need financial data in India to back our anti-money laundering laws. Data is safest in India.	

[253] P. Bhakta, India's data localisation policy will benefit the startup ecosystem: Paytm, September 20 2018, <https://tech.economictimes.indiatimes.com/news/internet/indias-data-localisation-policy-will-benefit-the-startup-ecosystem-paytm/65881255>

[254] PhonePe, Data Localization — Why this Kolaveri Di?, September 11, 2018, <https://blog.phonepe.com/data-localization-why-this-kolaveri-di-6d5680e3f012>

[255] M. Variyar, IAMAI & Nasscom raise concerns over India's draft data protection bill, September 5 2018, <https://tech.economictimes.indiatimes.com/news/corporate/iamai-nasscom-raise-concerns-over-indias-draft-data-protection-bill/65680064>

[256] Ibid.

[257] Mohandas Pai says payments data will be safe if stored in India, October 16 2018, <https://economictimes.indiatimes.com/tech/internet/mohandas-pai-says-payments-data-will-be-safe-if-stored-in-india/articleshow/66246707.cms>

42	Michael Dell, CEO, Dell Technologies [258]	Private Sector (Foreign)	For	Potential for abuse but could lead to greater digitisation, growth and innovation. More countries will follow.	
43	Victor Peng, CEO, Xilinx[259]	Private Sector (Foreign)	For	India generates a significant amount of unstructured data - localisation allows for data sovereignty.	
44	Ajay Banga, CEO, Mastercard[260]	Private Sector (Foreign)	Against	Prevents the learnings in one country from being applied in another or on global platforms.	
45	US-India Business Council[261]	Business Advocacy Organisation	Against (Regarding RBI Circular)	India must pursue policies to ensure that it remains a hub for global services.	
46	Arijit	Public	Against	The technical	

[258] V Mahanta, Dell acknowledges India's data concerns, expects ripple effect, October 17 2018, <https://economictimes.indiatimes.com/tech/internet/dell-acknowledges-indias-data-concerns-expects-ripple-effect/articleshow/66253989.cms>

[259] C.R. Sukumar, Data centres will grow on localisation move: Xilinx CEO, November 20 2018, <https://economictimes.indiatimes.com/tech/hardware/data-centres-will-grow-on-localisation-move-xilinx-ceo/articleshow/66701473.cms>

[260] S. Malviya, Localisation may not ensure data security: Mastercard chief Ajay Banga, November 1 2018, <https://economictimes.indiatimes.com/tech/internet/localisation-may-not-ensure-data-security-mastercard-chief-ajay-banga/articleshow/66456945.cms>

[261] Policies restricting data flow 'barriers' to growth of payments market in India: USIBC, October 16 2018, <https://economictimes.indiatimes.com/industry/banking/finance/policies-restricting-data-flow-barriers-to-growth-of-payments-market-in-india-usibc/articleshow/66249159.cms>

	Sengupta, VP - Public Advocacy,The Practice[262]	Relations Firm		ramifications of having core data stored within India has not been fully explored.	
47	Association of Corporate Counsel[263]	Global Legal Association	Against	"Serving copy" undefined. Restricting international data flow hampers law enforcement access.	
48	BSA, The Software Alliance[264]	Advocacy Group (Software Companies)	Against	Measure not adequately justified. Will effect country's economy and competition in this sector.	
49	Centre for Communication Governance [265]	Research Centre	Against	Does not prevent foreign surveillance or ensure law enforcement access to data.	Improving cross border access to data.
50	Submissions by Researchers		Against	State surveillance expands in the absence of	Failure to account for high ecological cost due to this

[262] Arijit Sengupta, Indian Personal Data Protection Act (IN-PDPA) 2018 – Distillation paper, <https://www.medianama.com/wp-content/uploads/Arijit-Sengupta-The-PRactice-Project-Submission-India-Draft-Data-Protection-Bill-Privacy-2018.pdf>

[263]https://www.acc.com/aboutacc/newsroom/pressreleases/india-data-protection-bill.cfm

[264] Comments of BSA | The Software Alliance on "The Personal Data Protection Bill, 2018" <https://www.medianama.com/wp-content/uploads/Business-Software-Alliance-Submission-India-Draft-Data-Protection-Bill-Privacy-2018.pdf>

[265] Centre For Communication Governance At National Law University Delhi, Comments On The Draft Personal Data Protection Bill, 2018 <https://www.medianama.com/wp-content/uploads/CCG-NLU-Submission-India-Draft-Data-Protection-Bill-Privacy-2018-and-Srikrishna-Committee.pdf>

	and Activists[266]			procedural safeguards.	initiative.
51	Internet Freedom Foundation (IFF)[267]	Collective (Advocacy)	Against	Require robust data protection rules irrespective of localisation. Open to third party abuse.	

[266] Solving for data justice: A response to the draft Personal Data Protection Bill Submission by Concerned People <https://www.medianama.com/wp-content/uploads/concerned-people-Submission-India-Draft-Data-Protection-Bill-Privacy-2018.pdf.pdf>

[267] Save our Privacy, A Guide To Participate In The Data Bill Consultation <https://www.medianama.com/wp-content/uploads/SaveOurPrivacy-Internet-Freedom-Foundation-Submission-India-Draft-Data-Protection-Bill-Privacy.pdf>