CARNEGIE INDIA

WORKING PAPER

APRIL 2021

How Would Data Localization Benefit India?

Anirudh Burman and Upasana Sharma

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

How Would Data Localization Benefit India?

Anirudh Burman and Upasana Sharma

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, D.C. 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

Carnegie India
Unit C-5 & C-6, Edenpark,
Shaheed Jeet Singh Marg
New Delhi - 110016, India
P: + 011 4008687
CarnegieIndia.org

This publication can be downloaded at no cost at CarnegieIndia.org.

CONTENTS

Introduction 1

History of Data Localization 3

The Case for Localization in India 7

Research Methodology for Evaluating Data Localization Proposals in India 10

Which Localization Measure Would Best Secure Data Access for Law Enforcement? 18

Which Localization Measure Would Best Spur Economic Growth? 24

Conclusion 29

Appendix 1: The Theoretical Underpinnings of the Criteria Weighting 31

Appendix 2: Measuring Law Enforcement Data Access and Data Localization 35

Appendix 3: Measuring Boosted Economic Growth and Data Localization 40

About the Authors 46

Acknowledgments 46

Notes 47

Introduction

Data localization has become a significant policy issue in India, as it has in many countries. Data localization refers to various kinds of policy measures that restrict the free flow of data across geographic boundaries. Countries limit such data flows in multiple ways. In some cases, firms are required to store a local copy of all data, even though this data can be taken and analyzed outside the country. In other cases, countries do not allow any data to be taken outside their territorial jurisdiction.

Over the years, the Indian government has passed sector-specific data localization measures, but now it is contemplating whether to pass a more expansive, economy-wide proposal. The Indian government has released multiple official reports and documents over the last five years that have articulated New Delhi's objectives for pursuing further data localization. Advocates for localization in India have highlighted the perceived economic benefits of processing Indian consumer data within the country, asserting that greater data localization would enable greater innovation and a larger producer surplus in the Indian economy. They also have noted the difficulties Indian law enforcement faces in accessing Indians' personal data stored outside the country to prevent crimes and pursue investigations. One especially noteworthy document, the Report of the Committee of Experts under the chairmanship of Justice B. N. Srikrishna, provided detailed reasons for proposing the localization of personal data in India.[1]

While some claim that keeping local data within a country's borders may result in economic and security-related benefits, this is not always the case. Multiple considerations determine whether a data localization measure has a net benefit on the localizing country. These considerations include the precise objectives that localization is meant to achieve, the specific localization measures implemented, the underlying economic context, and the country's national security apparatus.

It makes sense that data localization proposals should be tailored to the country in question and that the costs and benefits should be considered contextually. After all, localization is a significant departure from the existing design principles of the internet, which are premised on the free flow of data across borders. Historically, consumers across the globe have gained access to innovative digital products premised on free flows of data. While some argue that this arrangement increasingly does not benefit local producers, local consumers have benefited from the proliferation of services created outside their countries. Given all these considerations, localization in some cases might be disadvantageous to a host country overall, even if it meets its stated objectives.

In addition to articulating the government's reasons for considering more robust localization, the Srikrishna Committee also formulated a data localization legislative proposal in the form of the 2018 Draft Personal Data Protection Bill.[2] Based on this draft, the Indian government introduced its own 2019 Personal Data Protection Bill in parliament. This bill contains a framework for implementing data localization requirements across the entire Indian economy.[3] In parallel, other government departments and bodies have also articulated reasons for data localization.[4]

The Indian government's proposal to localize data must be evaluated on how well it would meet the government's multiple stated objectives. While there may be other reasons for and against data localization, understanding whether such a policy change would meet these democratically articulated objectives is an important starting point.

Crucially, it is important to understand what specific variant of data localization (if any) would best achieve the government's objectives. Rather than pose the broader question (as some studies have) of whether data localization would have a desirable overall impact on India's economy, trade, or citizens' privacy, the aim here is to examine what kind of data localization measure, if any, is best suited to meet the Indian government's objectives.[5] These include the aforementioned concerns over national security, domestic law enforcement, and economic growth.

This paper is structured to contextualize, measure, and analyze the likely effects of various data localization measures the Indian government could pass. First it gives the historical context of data localization globally and in India particularly. Next it provides an overview of the rationale for localization, its prevalence across jurisdictions, and the specific designs adopted in major jurisdictions. Third, the paper explains the multicriteria decisionmaking (MCDM) methodology adopted to understand what localization measures, if any, are best suited for the Indian context. The analysis of these localization alternatives is presented in the paper's fourth and fifth sections.

The research methods impose certain constraints on the precision of these findings. The research approach combines both qualitative and quantitative information on different aspects of data localization and seeks to create a ranking of localization alternatives. The scores provided in this analysis are therefore indicative of the *relative viability* of a localization measure, rather than an absolute judgment on its feasibility. In addition, while the suitability of data localization alternatives is analyzed with regard to two objectives (data access for law enforcement and economic growth), the paper does not provide an overall composite score or ranking for the data localization measures it considers.

This analysis contributes to the debate on data localization in multiple ways. First, this study analyzes the viability of localization alternatives from the perspective of the state. The study is based on the rationales the Indian government has given for pursuing such a policy. Second, the paper reaches

definitive conclusions on the viability of data localization with regard to certain officially stated objectives. Data localization, for example, would not enable access to data in cases when the data sought by Indian law enforcement is stored in another country and subject to foreign laws. This fact has important implications. The best way to establish jurisdiction over data seems to be to do so directly by establishing legal jurisdiction over firms that conduct business in India or to enter into international arrangements that allow hassle-free access to data. Data localization is unlikely to help India achieve objectives that actually require access to data. Law enforcement and national security objectives may instead be best served by a combination of light-touch localization requirements (such as mirroring requirements that mandate the storage of a local copy in India, while the data can be processed and stored globally) and bilateral and multilateral frameworks that enable India's access to data stored outside its jurisdiction.

Lastly, this paper finds that local storage requirements could promote India's stated objectives for spurring economic growth. Such requirements could drive up demand for goods and services in India, while also giving Indian firms a slight competitive advantage over their foreign peers. This calculus depends on various contingent factors, such as whether the resultant demand for data centers would be met by indigenous firms or through imports (which would not add to Indian gross domestic product, GDP), the adaptability of Indian firms to the costs of implementing localization, and the likelihood and severity of retaliatory measures by other countries on Indian service-sector exporters. However, data localization is not required to give Indian producers greater access to personal data for innovation. This is because, as stated before, localization does not by itself advance jurisdictional claims.

History of Data Localization

The introduction of the internet transformed the global economy, altered how businesses are organized, and changed how trade is conducted. It also led to a significant increase in technology-driven productivity. From 1992 to 2017, worldwide internet networks went from carrying 100 gigabytes (GB) of traffic per day to over 46.6 terabytes (or 46,600 GB) per *second*.[6] It is estimated that, by 2022, global online traffic will reach 150.7 terabytes per second.[7] The growth of cross-border data flows has benefited many small and medium-sized enterprises around the world. There is evidence that businesses that utilize the internet to trade globally have a higher survival rate compared to those that do not.[8] Simultaneously, the free flow of data via the internet has also allowed multinational companies to process large volumes of data across national boundaries. Free flows of data have spurred significant innovation and productivity gains globally for both small and large firms.

The Case for Localization of Various Stripes

However, as the digital economy expands, countries have expressed four key concerns over the free flow of data. These are: (1) storage of data on foreign servers, which has impeded data access for domestic national security agencies, (2) the loss of economic benefits due to exploitation of data by foreign firms, (3) concerns about foreign surveillance, and (4) misuse of personal data in violation of privacy rights.

These risks have led many countries to conclude that data flows must be regulated. Data localization is one such measure, and it is not a novel idea. Over the past two decades, many countries have implemented restrictions on the free flow of data. Many countries have adopted localization requirements in selected sectors or industries, such as for critical infrastructure or national defense.

There are different ways data localization can restrict data flows by limiting the physical storage and processing of data within a given jurisdiction's boundaries.[9] These measures can be broadly divided into two categories: hard and soft localization. Hard localization requires local storage and local processing of data. This form of localization does not allow for cross-border data transfers. Soft localization requires some form of local storage but allows data to be transferred and processed outside domestic borders if certain conditions are met. These two broad categories can be subcategorized more granularly. These include sector-specific localization, conditional localization, and general localization measures that can be exempted by bilateral or multilateral arrangements. Table 1 provides definitions of the main variants.

TABLE 1
Variants of Data Localization

Type	Definition
Sectoral	Data localization for a particular sector of the economy. These specific forms of localizatio;n sometimes can prevent data flows outside the country (hard localization) or other times can allow data flows with some restrictions (soft localization).
Conditional	Data localization whereby the storage, processing, and transfer of data is dependent on certain conditional prerequisites. For example, the Indian Personal Data Protection Bill, 2019 requires data to be localized if the central government deems it to be critical personal data. This type can have both hard and soft localization variants as well.
Bilateral/Multilateral Agreements	Data localization measures that are dependent on bilateral and multilateral agreements that participating countries have entered into. Countries can potentially have a general framework requiring data localization and provide exemptions to specific countries or groups of countries.

SOURCE: Typology developed by the authors.

Different countries (and blocs) have employed data localization of varying designs, sometimes across their entire economies and sometimes within specific economic sectors. One of the most significant pieces of legislation on data flows is the European Union's (EU) 2018 General Data Protection Regulation (GDPR), which imposes conditions on the free flow of data affecting all EU member states.[10] China, meanwhile, requires that all "important data" concerning "critical information infrastructure" be localized.[11] Similarly, Russia requires all personal data of its citizens to be locally stored.[12] Other countries have taken other approaches. The United States requires that all defense-related data be locally stored. For its part, Indonesia requires that all information related to public services be localized.[13] Table 2 provides a summary of major countries that have employed localization measures.

TABLE 2
Data Localization in Major Countries/Blocs

Country/Bloc	Localization Type	Sectors	Relevant Law
China	Unconditional	Covers all sectors. Applies to critical information infrastructure and "important" personal information of any natural person collected or produced by public communication and information services, transport, energy, finance, or the government[14]	Article 37 of China's Cybersecurity Law[15]
Indonesia	Unconditional	All public services	Information and Electronic Transaction Law[16]
Russia	Unconditional (mirroring)	All personal data of Russian citizens	Federal Law No. 242 - FZ[17]
Australia	Unconditional (sectoral)	Sensitive personal health data	My Health Records Act, 2012[18] (amended in 2018[19])
United States	Unconditional	Critical information for operational security and national defense	Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018)[20]
EU	Conditional transfers	All personal information	General Data Protection Regulation (GDPR)[21]

Countries have tried to simultaneously regulate the flow of data across territorial boundaries by way of international frameworks. As table 3 shows, many bilateral and multilateral frameworks involve countries promising to adhere to similar standards on personal data protection. In addition, they also agree to facilitate the exchange of information needed for critical national security or law enforcement purposes. Such agreements allow signatory countries to lower data localization requirements for each other.

TABLE 3

Major Bilateral, Multilateral, and Legislative Arrangements on Data Localization

Name of Data Localization Agreement/Measure	Countries Involved	Purpose
The Clarifying Lawful Overseas Use of Data (CLOUD) Act[22] *(2018)*	U.S. domestic legislation. Participating countries: United Kingdom	Facilitates countries gaining access to stored foreign data in a timely manner through executive agreements wherein both the U.S. and the foreign governments "share a common commitment to the rule of law and the protection of privacy and civil liberties."[23]
Osaka Track[24] *(2019)*	A plurilateral initiative started by Japan	A plurilateral framework that promotes cross-border data flow with enhanced protections among twenty-four countries and groupings.[25]
APEC Cross-Border Privacy Rules System (2005)	United States, Canada, Mexico, Japan, Singapore, Taiwan, Australia, the Philippines, and South Korea	Facilitates a framework for cross-border data transfers specifically for countries in the Asia-Pacific.[26]
United States-Mexico-Canada Agreement (2020)	United States, Mexico, and Canada	Facilitates the free flow of data between the United States, Mexico, and Canada with privacy and security safeguards.[27]
Comprehensive and Progressive Agreement for Trans-Pacific Partnership (2018)	Member countries: Canada, Australia, Brunei, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam	Specifically prohibits localization requirements among signatories.[28]
Digital Economy Agreement (DEA), (2020)	Member countries: Singapore, Australia	Specifically prohibits data localization for Australian businesses in Singapore and vice versa.[29]

The Case for Localization in India

Before considering the recent localization measures the Indian government is contemplating, it is helpful to give a snapshot of what the country has done so far. Like some other countries, India has already adopted a patchwork of data localization measures in some economic sectors. For example, the Reserve Bank of India requires all payment data to be stored in India, though it can be taken out of the country for processing.[30] Another sector-specific measure in the telecommunications sector requires local storage and local processing of subscriber information and prohibits the transfer of accounting information related to subscriber or user information.[31]

Table 4 chronologically lists the major sector-specific localization measures already in effect in India. As the table shows, many sectors of the Indian economy already require data localization, mostly by way of local storage of consumer data.

TABLE 4
Sectoral Data Localization in India

Sl. No	Act/Initiative	Year Implemented	Mandate
1	Public Records Act[32]	1993	Prohibits the transfer of any "public records" outside India.[33]
2	Information Technology (IT) Act in 2000,[34] and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011	2000 and 2011	Prohibits the transfer of sensitive personal data by a body corporate outside the country unless the other party can match the same level of data protection mandated under the IT Rules.[35]
3	Unified Access License for Telecom Service Providers	2004	Requires local storage and local processing of subscriber information and prohibits the transfer of i) accounting information related to the subscriber and ii) user information.[36]
4	National Data Sharing and Accessibility Policy (NDSAP)[37]	2012	Mandates localization of all government-related data,[38] and allows sharing of all nonsensitive data for "legitimate and registered use."[39]
5	Companies Act, 2013	2013	Requires local storage of the books of accounts of Indian companies (including books and papers stored in electronic modes)[40]

6	MeghRaj Initiative (an Indian government initiative with respect to data storage practices of government departments and authorities)	2014	Requires that all empaneled cloud service providers store "the data center facilities and the physical and virtual hardware"[41] only in India.
7	National Telecom MDM Roadmap[42]	2015	Requires all M2M gateways and application servers "servicing customers in India to be physically located in India."[43]
8	FDI Policy 2017[44]	2017	Requires all FDI-receiving entities in the broadcasting sector to ensure local storage and processing of subscriber data. It also prohibits transfer of subscriber data outside India.[45]
9	The IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017	2017	Mandates local storage of original payholders' accounts.[46]
10	Reserve Bank of India Storage of Payment System Data	2018 and 2019	Mandates local storage of payments data; the clarification issued in June 2019 mentions that the processing of data may be done abroad, but the final copy will be stored in India.[47]

SOURCE: Compiled by the authors

The analysis in the rest of this paper assesses whether the *additional* data localization measures in the proposed 2019 bill are suitable for achieving the government's stated objectives. Now, as the Indian government considers a more robust, all-encompassing bill on data localization, it is important to assess the likely effects of such a policy in terms of the objectives it would be designed to meet. The Justice Srikrishna Committee proposed data localization in the 2018 Draft Personal Data Protection Bill it prepared as a part of its report. It provided a cross-sectoral data localization requirement, with escalating levels of restrictions on the flow of personal data, sensitive personal data, and critical personal data, respectively. The Indian government modified this proposal in the 2019 Personal Data Protection Bill, which was introduced in the Indian parliament. The most significant change was that a larger volume of data would be allowed to flow freely across Indian borders.

The bill proposes that localization measures be adopted across all sectors of the Indian economy for specific categories of personal data. If the bill is passed, all data not deemed "sensitive" personal data or "critical" personal data could be moved out of India freely. Categories of data defined as sensitive personal data could only be taken out of the country if certain conditions were met, and this data would have to be stored in India once processed. Critical personal data could not be taken out of

India except under very limited circumstances. The bill does not define critical personal data and leaves it to the central government to define such data categories, but the terms have not been publicly defined yet.

Any analysis of India's data localization proposals must begin with the government's four stated objectives: (1) securing speedier and better access to personal data for law enforcement, (2) increasing economic growth, (3) preventing foreign surveillance, and (4) helping enforce data protection laws.

On the national security front, Indian law enforcement agencies face difficulties when the personal data of Indian residents is stored outside the country. The Justice Srikrishna Committee report states that access to personal data for law enforcement agencies is one of the primary considerations for requiring data localization. For example, it explicitly cites the local storage of data as a means of facilitating speedier access to data for law enforcement agencies.[48] The document also highlights the importance of speedy access to data for national security purposes.[49] This thorny issue came to the forefront when fake news circulating on WhatsApp in various parts of India resulted in mob violence against innocent individuals.[50] In many such cases, police needed information on the origin and content of the messages, which were (and continue to be) encrypted. The Indian government wants to exercise greater regulatory supervision over social media services like WhatsApp. Some observers have posited that data localization would enable Indian authorities to do so.

In various government documents, New Delhi also makes it clear that fostering greater economic growth is a key consideration, one that must be evaluated on how well it increases innovation, and also the demand for data-related goods and services within India.[51] To this end, it has also been claimed that data localization will enable local IT businesses to innovate and compete with large technology firms. We therefore have to assess whether data localization measures enable innovation and provide competitive advantages to such local businesses.

In addition, the Justice Srikrishna Committee's report states that data localization is essential to protect Indians from foreign surveillance.[52] Similarly, the draft National E-Commerce Policy Report also anticipated the role of localization in preventing foreign surveillance.[53] In 2013, Edward Snowden, a former U.S. contractor for the Central Intelligence Agency, disclosed that the United States' National Security Agency was surveilling the communications of foreign governments and citizens. This revelation highlighted the extent to which digital surveillance could be conducted.[54] Simultaneously, the internet has also facilitated a steady increase in the scale and scope of cyber attacks.[55] In 2020, a World Economic Forum survey ranked cyber crime as the "second most concerning risk for doing business globally" over a ten-year horizon.[56]

Finally, the committee's report argues that data localization would enable India to maximize the economic potential of the vast troves of personal data the country has generated.[57]

But the report does not provide any evidence for any of these four claims, based on which it advocates data localization. Lastly, the committee's report also discussed efforts to better enforce data protection laws through the creation of a Data Protection Authority.[58]

These are the four government-stated objectives that this analysis examined to gauge the potential impact of an economy-wide data localization law in India.

Research Methodology for Evaluating Data Localization Proposals in India

To restate the paper's central inquiry, the specific design of the localization measure in question must be evaluated based on how well it would help the Indian government meet its stated objectives. To do so, this analysis employs MCDM methods. These methods are useful for considering multiple alternatives by ranking them on selected criteria. This method has been used previously for evaluating policy alternatives in a diverse range of fields such as energy, the environment, sustainability, supply chain management, infrastructure, and others.[59]

To apply MCDM methods to the case of Indian data localization, it is necessary to follow these seven steps:

- clearly define the relevant independent variables (the Indian government's desired objectives for pursuing data localization)
- clearly define the range of relevant dependent variables (in this case, the different data localization measures the Indian government could adopt)
- identify clear, objective criteria for evaluating the relative merits of India's various localization options in terms of the government's stated objectives
- design a suitable scale to measure the goal-based criteria and weight them appropriately so that the effects of the localization policy variants can be compared to a standardized scale
- set the baseline scenario based on the current status quo and state the study's operative hypothesis
- assign each policy option's scores for each defined criterion by assigning a value from the ten-point scale and properly weighting its value
- tabulate each policy option's total score to evaluate its overall merits in a holistic way

The authors hypothesized that each objective articulated for localization would be achieved best depending on what *specific* kind of localization measure is adopted. They expected that an assessment of each alternative based on specific relevant criterion would help identify which kinds of localization measures, if any, are best suited for achieving India's objectives. At this stage of the analysis, the running hypothesis was that more free flow of data would be better for economic growth, while law enforcement objectives could be met by complementing the free flow of data with bilateral and/or multilateral agreements that enabled data access for law enforcement agencies.

Identifying the Indian Government's Stated Goals

The first step is to identify and define the Indian government's objectives precisely. As explained in the previous section, the following four objectives have been articulated in multiple Indian government documents.

- securing faster and better access to personal data for law enforcement
- spurring increased economic growth and employment
- preventing foreign surveillance, and
- better enforcing data protection laws

The authors studied each objective to analyze whether any form of data localization would help meet these stated objectives and realized that data localization does not enable governments to achieve the last two objectives.

The prevention of foreign surveillance is a legitimate objective of every sovereign state. Nation-states are interested in preventing the surveillance of certain categories of individuals such as senior government officials, defense personnel, and sensitive scientific research personnel. In India, data localization measures are already in place with respect to government data and communications, so further measures to protect their data would be redundant.[60]

Therefore, the scope of the debate on the efficacy of data localization for preventing foreign surveillance pertains to personal data that is not already subject to the regulatory requirements and other steps mentioned above. This personal data could possibly include the personal data of government officials generated while they act as private citizens outside the scope of their employment. However, their personal data on social media platforms and other online businesses may be accessed legally by foreign governments (as per the law of the foreign government) if such data is stored within the jurisdiction of foreign governments.

Even if such data is stored locally, and if foreign governments are determined to access such information, they would do so through mechanisms that make data localization redundant as a security

measure. Data security and confidentiality are increasingly guaranteed through data security features other than data localization.[61]

With regard to the enforcement of data protection laws, as Basu et al. note, alternative approaches to localization for improving the enforcement of IT law are already in place in India.[62] Enforcement of Indian law is ensured through local incorporation and establishment requirements, rather than requirements that businesses locate physical infrastructure in India. Under the proposed data protection law, the enforcement of data protection laws would be contingent on foreign businesses establishing a business presence in India, not on data localization. The bill requires significant data-related businesses (significant data fiduciaries) to register in India. The enforcement of data protection law against such businesses would therefore be a product of their legal registration in India rather than data localization stipulations.

For these reasons, the paper's assessment of localization measures was confined to the achievement of the first two objectives: securing faster and better access to personal data for law enforcement and spurring increased economic growth and employment.

Once these objectives were clearly defined, the requirements for achieving them were disaggregated and defined based on secondary research and discussions with stakeholders.[63]

For law enforcement's access to data, the following considerations came into play.

- Crime prevention:
  - Accessing encrypted data could help law enforcement prevent crime by monitoring possible offenders
  - Monitoring of suspects' social media accounts and financial activities using digital data can help law enforcement track financing for terrorism and prevent attacks

- Investigation of crimes:
  - Gaining faster access to data would help law enforcement investigate crimes more rapidly
  - Getting access to GPS data could help law enforcement locate suspects and criminal offenders
  - Securing broader access to financial data could aid law enforcement in money laundering investigations.

- Economic objectives
  - Gaining access to data sets already available with foreign businesses could help give Indian firms a competitive advantage in fields like artificial intelligence (AI)

- Making data more available could help lower barriers to scientific innovation for smaller Indian companies
- Enacting data localization stipulations would likely produce economic benefits and create jobs for more people in India, including both temporary and permanent positions (in data center management, AI, and other industrial applications, for example)

Identifying the Different Localization Variants

After defining the Indian government's objectives, the authors identified four different, mutually exclusive variants of data localization measures that the Indian government could adopt (see table 5). These include: (1) some form of conditional localization through data mirroring or local storage requirements for critical personal data, (2) unconditional local storage requirements for all personal data, (3) unconditional mirroring requirements for all personal data, or (4) the unconditional free flow of data accompanied by bilateral and multilateral agreements for managing data access and transfers. These four broad alternatives are categorized by the stringency of local storage requirements and the scope of personal data that must be localized.

The authors then further disaggregated these variants into stylized models of more specific forms their localization measures could take. While many more variations are theoretically possible, the focus here is on the ones deemed most feasible given the current legislation that the Indian parliament is considering.[64]

TABLE 5
Categories and Corresponding Alternatives of Data Localization

Localization Variants	Granular Data Localization Alternatives
A conditional localization requirement that could entail either mirroring or local storage requirements (for critical personal data only)	a) Conditional mirroring: This option would entail global storage and processing of data with a requirement for local mirrored copies (only for critical personal data) instead of full local storage and processing requirements. b) Conditional soft localization: This alternative would involve local storage and global processing only for critical personal data, and otherwise would be similar to the previous alternative. However, this option would allow personal data to be taken out of India for processing. c) Conditional hard localization: This option would entail local storage and processing, but only for critical personal data. This alternative assumes that the baseline scenario applies to normal personal data, but certain sectors of the economy and certain kinds of data would be subject to hard localization requirements. This framework is proposed in the parliament's bill with respect to critical personal data.

Localization Variants	Granular Data Localization Alternatives
Unconditional local storage requirements (for all personal data)	a) Hard localization: This alternative would require local storage and processing for all personal data. This does not represent the government's current position in the Indian parliament's bill, which would apply to critical personal data only. However, this assumption of complete data localization offers a clearer comparative picture for assessment purposes. The scores for this alternative must therefore be considered accordingly. b) Local storage with global processing: This option would allow local storage, though processed data would have to be kept in India. This approach would mean that all personal data generated in India would have to be stored in India but could be taken out of India for processing. This policy measure is the one that would be applied to sensitive personal data under the parliament's current bill.
Unconditional mirroring requirements (for all personal data)	a) Free flow of data with mirroring (with MLATs): This alternative would mean global storage and processing of data with local mirrored copies and the use of mutual legal assistance treaties (MLATs). This approach adds a minor impediment to the baseline scenario by requiring that a copy of all data be mirrored in India. All other parts of the baseline scenario remain the same. b) Free flow of data with mirroring (with bilateral/multilateral frameworks): This option would entail global storage and processing of data with local mirrored copies and the use of bilateral or multilateral frameworks for data access. In this variant of the mirroring alternative, mirroring would be required even if India enters into bilateral or multilateral agreements for data sharing and access.

Localization Variants	Granular Data Localization Alternatives
Unconditional free flow of data with bilateral/multilateral agreements for data access and transfers	a) No localization (global storage and processing of data, with MLATS): This alternative would mean global storage and processing of data plus the use of MLATs. This is the baseline scenario that reflects the existing policy landscape as of today. Other than sectors that already have their own localization requirements, there are no economy-wide data localization requirements in India. Law enforcement access to data stored abroad takes place through the MLAT process. Under the current version of the Indian bill being considered in the parliament, this baseline scenario would continue to apply to all personal data that is not deemed sensitive or critical. India could possibly enter into international agreements for access to such data in the future. This eventuality is considered in the next alternative. b) No localization (global storage and processing of data with bilateral/multilateral agreements for data access): This option would involve global storage and processing of data with bilateral or multilateral frameworks for data access. It would be an improvement on the baseline scenario where data access issues created by jurisdictional conflicts are resolved through MLATs. The authors assume that such bilateral or multilateral agreements would allow Indian law enforcement access to both content and noncontent data in all cases of serious criminal investigations and prosecutions. Under such agreements, the operating assumption is that the Indian government would be able to seek data access directly from companies without having to go through a diplomatic or judicial process in the host country. Similarly, for data access for commercial purposes, the authors assume that data access under these agreements would require minimal compliance and that adequacy requirements for data protection, if any, would be liberally construed. It is worth noting that this assumption does not reflect the dominant bilateral or multilateral agreements, which limit law enforcement's access to certain kinds of data, or cross-border data sharing for commercial purposes.[65] This paper adopts a simplified model of international frameworks to streamline the analysis and to provide a better understanding of how a framework that resolves all jurisdictional conflicts compares to others. The scores for these alternatives must therefore be considered accordingly. Even so, these assumptions provide the advantage of considering the maximum benefits available under a framework in which no localization is required and data access across jurisdictions is frictionless. This stylized framework is helpful in comparing such a regime with one that requires cross-sectoral hard localization. Under the bill the parliament is currently considering, data access and transfer issues could conceivably be resolved through international agreements. However, this would not be the case for critical personal data.[66]

Identifying Criteria for Evaluating India's Various Localization Options

After laying out these localization alternatives, the authors identified relevant criteria by which to assess their relative efficacy in meeting the government's objectives. This task was done by using the aforementioned information to disaggregate the government's two key objectives: improving law enforcement's data access and spurring economic growth.

Four criteria were identified for assessing which alternative would best meet the objective of improving law enforcement's access to data: (1) the scope of access, (2) the speed of access, (3) the risk of foreign retaliation against Indian firms abroad, and (4) the risk of data loss due to foreign firms exiting India amid heightened regulations. Similarly, four separate criteria were isolated to gauge how readily each localization variant would spur economic growth: (1) demand for goods and services, (2) competitive advantages for domestic producers and competitors, (3) the risk of data loss due to foreign firms exiting India amid heightened regulations, and (4) the risk of foreign retaliation against Indian firms abroad.

A more detailed explanation for each of these criteria is given in the next section of the paper.

Measuring and Weighting the Goal-Based Criteria

To score each of the potential localization alternatives, the authors first used a ten-point scale for each of the evaluating criteria (with ten being the scale's highest value and one being the lowest). When gauging both law enforcement access and economic growth, two of the criteria—the risks of retaliatory action and of data loss—the scoring method was flipped. More specifically, the localization alternative posing the highest risk received the lowest score (zero) and the alternative posing the lowest risk scored the highest (ten). The authors chose to make this adjustment so that the scoring of the positive variables (data access and heightened demand, for instance) moved in the same direction as the negative variables (retaliatory and data loss risks) rather than at cross purposes.

Once the scales were established, the next step was to assign a weight to each criterion. To do so, the authors created a pair-wise comparison matrix where each criterion was measured against itself and the other criteria. This exercise was conducted for all the criteria separately for assessing law enforcement's data access and the prospects for spurring economic growth. A detailed rationale for the usage of this scale is given in appendix 1 based on the methodology developed by Saaty.[67]

In the end, the various criteria were weighted in the following way. When gauging law enforcement's access to data, the scope of data access was weighted at 31 percent, the speed of access was assigned 50 percent, the risk of retaliatory action against Indian firms abroad was listed at 5 percent, and the risk of data loss came in at 14 percent. On the question of spurring economic growth, heightened demand for goods and services was weighted at 36 percent, any competitive advantage accrued by

domestic producers or competitors came in at 38 percent, the risk of data loss stood at 18 percent, and the risk of retaliatory action amounted to 18 percent. See appendix 1 for a full explanation of how these weightings were determined. Based on this ten-point scale and weighting system, the authors ranked all the criteria relative to each other and weighted them accordingly.

Setting the Baseline and Stating the Operative Hypothesis

Before the various policy options were scored, we decided to use India's existing legal framework on localization as a baseline case to measure the potential alternatives against. To review briefly, the legal status quo does not impose localization requirements (except in specific, limited sectors) on the flow of data, and law enforcement agencies use MLATs to request access to data stored abroad. Other alternatives were scored in relation to this baseline scenario. The baseline scenario is therefore listed as alternative A1 in both appendixes 2 and 3 (which provide the detailed scoring and rationale for each policy alternative's scoring).

Scoring Each Localization Policy Option

Scores for each localization alternative were assigned according to a simple calculation: each policy's assigned value on the ten-point scale times the assigned weight of that criteria weight. We provide an example of this below using the alternative "No localization: global data storage and processing with MLATs" from the law-enforcement objective. In each box below, the first number multiplied is the policy option's score on the ten-point scale multiplied by a second number representing its assigned weight. On scope of data access, for instance, the policy option of no additional localization was assigned a score of six out of ten, and this value was multiplied by 31 (for its 31 percent weighting) to get a total of 186. The aggregate score in the final column on the right represents the tabulated total of these four composite scores. (See appendix 2 for a detailed rundown of how each of the policy options were scored in terms of granting law enforcement data access and appendix 3 for a rundown of how they were scored in terms of spurring economic growth in India.) Other alternative localization measures would score higher or lower than six out of ten on scope of data access, three out of ten on speed of data access, nine out of ten on the risk of retaliatory action, and nine out of ten on the risk of data loss, all numbers that affect the aggregate weighted scores.

Localization alternative	*Scope of Data Access (31%)*	*Speed of Data Access (50%)*	*Risk of Retaliatory Action (5%)*	*Risk of Data Loss (14%)*	*Aggregate Score*
No localization: global data storage and processing with MLATs	6 x 31 = 186	3 x 50 = 150	9 x 5 = 45	9 x 14 = 126	507

Tabulating Each Localization Policy's Total Score

For each policy alternative, the authors added up the weighted scores in each criteria column to assign an aggregate score (the farthest-right column in the example above). This process was done twice for each policy alternative, once to measure its efficacy in terms of giving law enforcement data access and again to measure its effectiveness in spurring economic growth. The alternative with the highest aggregate score compares most favorably to other localization alternatives and is the most likely to achieve the stated policy objectives: improving law enforcement access to data or fostering economic growth and innovation, while balancing countervailing risks.

Which Localization Measure Would Best Secure Data Access for Law Enforcement?

Lacking timely access to data held overseas can be a major constraint on Indian law enforcement personnel when conducting investigations. This is usually because the data law enforcement is seeking was collected in India and stored in another jurisdiction, leading to a conflict of legal systems. While MLATs can offer access to personal data in such situations, this cumbersome process often takes around ten months on average in all cases.[68] Mandating local data storage and processing through localization would not necessarily solve this problem since businesses can still be bound by the laws of their home country even if they store their data in India.[69]

Indian law enforcement also faces issues with getting access to *different kinds* of data. Laws in other countries prohibit their businesses from sharing certain kinds of data with investigative authorities in other jurisdictions.[70] One argument for data localization is that it will resolve both issues for law enforcement agencies by enabling faster access to different kinds of data.

To measure which localization alternative would best help law enforcement get improved access to personal data, the authors assessed the scope and speed of data access and the risks of foreign retaliation against Indian firms abroad and of data loss stemming from foreign firms ceasing operations in India to escape heightened regulations.

Two criteria (scope of data access and speed of data access) were clearly more important for the fulfillment of this objective and therefore received a significantly higher weighting (31 and 50 percent, respectively) relative to the others. Of these, the speed of data access has been clearly highlighted to be more important in multiple documents.[71]

The countervailing risk of data loss due to foreign companies leaving India receives a much lower weighting (5 percent). While India does face a risk of losing foreign businesses, India is also a large market, and foreign investments into technology have continued to flow into the country despite localization already mandated in some sectors, and the impending prospect of localization under the Personal Data Protection Bill. While it is logical to assume that localization would increase compliance costs and lead to firms leaving India, this has not been borne out by evidence. Technology FDI has continued to pour into India despite the increased threat of localization. In 2020, India received its highest ever FDI inflows, mostly into the technology sector.[72] Therefore, while this analysis considers the possibility of losing business due to localization, recent evidence shows that the likelihood of this occurring is extremely low. This criterion is therefore accorded a very low weight compared to the two previous criteria.

Similarly, while there is a real threat of retaliatory action by foreign governments, this would be a minor consideration in terms of Indian law enforcement's overall stated objective of receiving greater data access, so that criterion is weighted accordingly (14 percent). While there is a real and possible threat of retaliatory action, the only recent such measure has been the measures the United States adopted in response to China's new national security law. There have been no other occurrences of retaliatory action in response to a localization measure. Therefore, this criterion is assigned a low weight based on the low probability of such actions materializing.

Scope of Data Access

Since Indian law enforcement's limited access to certain kinds of data (specifically content data) held overseas is a key constraint on law enforcement personnel's ability to perform their duties, the authors measured which localization variant would grant them access to the largest variety of personal data. At present, the status quo (see alternative A1 in appendix 2) means that foreign firms are not allowed to share content data, which is data that is identifiable to a specific user.[73] U.S. companies currently hold most of the personal data in the world, and therefore the main counterparts on questions of access to such data are U.S. businesses.[74] Because of an exception under the U.S. Electronics Communications Privacy Act, U.S. businesses voluntarily provide noncontent data to Indian law enforcement.[75] This practice would continue regardless of which option India chooses.

Consequently, Indian law enforcement also has been increasingly requesting access to encrypted data.[76] Yet mere localization is not likely to significantly increase the scope of data available to Indian law enforcement mainly because of a conflict between Indian and U.S. law.[77] A U.S. law known as the Stored Communications Act (SCA) prohibits businesses from sharing personal data with any foreign government unless certain legally mandated procedures are followed. Only certain kinds of data (noncontent data or subscriber information) can be shared with foreign law enforcement

without undergoing this process. That means that, with respect to Indian data captured by U.S. businesses, the scope of accessible data for Indian law enforcement does not and will not vary significantly based on which localization measures are enacted. The scope of India's data access may, however, vary in relation to other countries (apart from the United States) that do not have similar blocking statutes.

Because of this, Indian law enforcement's access to personal content data would increase the most if India enters into a bilateral or multilateral framework because these frameworks would specifically enable law enforcement's access to an increased scope of data (see alternatives A2 and A4 in appendix 2). The status quo baseline scenario is clearly suboptimal because of the inefficiency of MLATs (see alternative A1 in appendix 2). India could also make modest gains by imposing restrictions on the flow of sensitive or critical personal data (see alternatives A7, A8, and A9 in appendix 2). This is because, while data currently located in non-U.S. jurisdictions is theoretically easier to access if such restrictions are imposed, data stored in the United States would continue to be as inaccessible as it is right now. These limited gains could also be significantly impaired if non-U.S. jurisdictions implement laws similar to prevailing U.S. law.

In short, Indian law enforcement will not be able to access foreign-controlled encrypted data by requiring localization. Doing so would require a legal mandate for decrypting data. Foreign businesses who wish to continue to provide services to consumers in India would comply with this legal mandate irrespective of whether they are asked to localize data.

Speed of Data Access

Since speedy access to personal data is such a key requirement for law enforcement investigations, speed of access outweighs other considerations by a significant margin in this analysis.[78] Both preventing crime and investigating past crimes require quick access to relevant information, and delays can drastically reduce the likelihood of success.

Under India's legal status quo (see alternative A1 in appendix 2), Indian law enforcement must first ask a business for information about an individual. A business that is subject to U.S. law must then consider whether it is has the information sought and crucially whether it is permitted to share such information with Indian law enforcement. If the information is content data and therefore subject to U.S. law, Indian law enforcement is asked to file an MLAT request.[79] If the MLAT request is directed to the U.S. government, the U.S. Department of Justice reviews the request and then a prosecuting attorney presents the request before a U.S. federal judge. If the judge agrees that the request meets U.S. judicial standards for sharing that information, the court issues an order for the business to share such information. As previously noted, on average this process takes a minimum of ten months.

While some form of local storage mandate might increase the speed with which Indian law enforcement gains access to data collected by non-U.S. businesses, it would not affect the aforementioned legal process for accessing content data from the United States (see alternatives A5–A9 in appendix 2). When it comes to data controlled by non-U.S. businesses, the speed of access for Indian law enforcement under all potential local storage alternatives is essentially the same, but that does not hold true for data controlled by U.S. firms. EU law, for example, does not contain provisions like those in the U.S. SCA.[80] Therefore, data collected by a business that is subject to the EU's GDPR could be accessed faster if the Indian government were to impose a localization mandate. This is subject to the EU's existing legal framework remaining static. However, the best alternative available for securing Indian law enforcement speedy access to content data is to enter into multilateral/bilateral agreements that overcome jurisdictional conflicts over data (alternatives A2 and A4 in appendix 2).

Data localization is likely to be insufficient for speeding up Indian law enforcement's access to personal content data. Other than entering into bilateral or multilateral frameworks, Indian policymakers can consider establishing local licensing requirements that would ensure that foreign businesses incorporate in India as subsidiaries or foreign branches and that the legal liability for collecting and storing Indian data rests with such Indian entities. For example, the Reserve Bank of India's localization requirement on payment-processing businesses and other financial firms is enforceable primarily because these entities cannot provide services in India without the Reserve Bank's prior authorization.[81] Securing such authorization in turn requires them to register as Indian entities.[82]

This is also how the United States exercises jurisdiction over data stored by its companies in other countries. The SCA enables the U.S. government to access data stored outside the United States by U.S. companies.[83] By making a claim of legal jurisdiction and regulating U.S.-based businesses, the U.S. government can require access to data if such data is in the company's "possession, custody or control, regardless of whether such . . . information is located within or outside of the United States."[84]

The Indian government may also therefore consider establishing legal jurisdiction to access data from businesses that provide services in India. The 2019 Personal Data Protection Bill provides for the registration of "significant data fiduciaries" in India.[85] However, it is unclear whether this registration will be a form of licensure and authorization to conduct business in India, or a registration of the service. The former would enable the Indian government to exercise greater jurisdictional control over the businesses that collect and store data on Indian citizens, in a manner similar to U.S. law.

Risk of Data-Holding Foreign Businesses Exiting India

Foreign businesses could react negatively to any further localization requirements India may institute for two reasons: escalating compliance costs and perceived privacy concerns. Any decision such firms may make to stop providing services in India due to compliance costs would involve a careful consideration of the benefits businesses would lose as well. India's digital economy is growing rapidly. Moreover, India is the world's largest accessible data market, and an extremely competitive one at that. These benefits would have to be weighed against any compliance costs to be incurred by businesses due to localization requirements.

Privacy concerns could also pose another serious reason for foreign businesses. U.S. and EU businesses are affected not just by shareholder concerns over consumer privacy but also by laws in these jurisdictions that place a great deal of weight on consumer privacy even in foreign jurisdictions.[86] For example, the United States has been ramping up pressure on its businesses providing services in China after a new Chinese national security law was passed in 2017.[87] These contextual and political considerations will also depend on the quality of bilateral relationships between India and countries like the United States.

If foreign businesses stop providing services in India for either of these reasons, the Indian economy would lose the benefits of these services, especially platform services that enable buyers and sellers to conduct e-commerce. More significantly from the perspective of meeting this objective, Indian law enforcement would lose access to the personal data of consumers already collected by such businesses since they would no longer be operating in Indian territory.

It is likely that, in some cases, an Indian business may crop up to provide similar services to Indian consumers, and the loss of the data and services could thus be mitigated. However, this process would take time and may not occur in all circumstances. For example, when the Indian government banned the Chinese social media app TikTok, user engagement on alternative apps remained much lower: As one Indian observer put it, "although TikTok users shifted to other alternatives, user engagement indicators such as app open rates and average session times are yet to catch up with TikTok's engagement levels."[88] This could be either because Indian substitutes do not exist, or because Indian competitors may be unable to replicate the same quality of service.[89]

This analysis therefore assigns the highest scores to localization alternatives that pose the least risk of driving away foreign businesses. Alternatives that do not impose a local storage restriction would pose fewer risks (alternatives A1–A4 in appendix 2) than ones that do. Therefore, even alternatives that impose mirroring requirements but do not otherwise restrict the flow of data score high on this criterion. Conditional localization requirements (alternatives A7–A9 in appendix 2) score the lowest

since, by definition, they restrict the flow of data that is considered more sensitive. In addition, the compliance requirements for segregating classes of data depending on their sensitivity is also higher than those of unconditional localization.

Risk of Foreign Retaliation Against Indian Firms Abroad

The analysis also measures the risk of other countries retaliating against localization measures taken by India. Such actions might lead other countries to impose localization restrictions of their own on Indian firms that export services and could negatively affect Indian data-related businesses that serve consumers in these jurisdictions. For example, the U.S. government issued an executive order banning TikTok on the grounds that "TikTok automatically captures vast swaths of information from its users, including Internet and other network activity information such as location data and browsing and search histories. This data collection threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information."[90]

Retaliatory measures could also involve measures that are not directly related to data. Countries that may adopt such measures are those with significant exporters of data-related services to India, including the United States.[91] Respondents in a November 2019 survey of Indian businesses by the Indian Council for Research on International Economic Relations said that there is a fear of retaliatory action against Indian IT companies that use "*off-shore models using citizen data of other countries*."[92] Such retaliatory measures would likely be stronger if India adopts stringent data localization measures.

More stringent and comprehensive localization measures therefore carry higher risks of retaliatory action. Unsurprisingly, alternatives that allow for the free flow of data score the highest. These options pose the lowest risks of retaliatory action (alternatives A1 and A2 in appendix 2). Unconditional hard localization poses the highest risk of retaliatory action (alternative A6 in appendix 2).

Overall Assessment

The aggregated scores on these individual criteria provide a final ranking of the data localization alternatives India is considering.[93] The current status quo whereby Indian law enforcement seeks and receives access to data through MLATs is clearly suboptimal (alternative A1). Localization measures that allow the highest degree of free-flowing data through a bilateral/multilateral framework for data access receive the highest aggregate scores (see alternatives A2 and A4 in appendix 2). A regime for free-flowing data supported by bilateral/multilateral agreements would enable Indian law enforcement to resolve the issue of conflicting legal regimes and expedite access to data. In addition, it

would also mitigate Indian law enforcement's current inability to access different kinds of data due to legal restrictions in foreign jurisdictions.[94] The model of multilateral/bilateral arrangements considered here does not reflect actual international agreements, which are either limited in the scope of data covered or allow free-flowing data for specific purposes.[95] This analysis provides a framework for thinking about the tradeoffs between free-flowing data versus localization restrictions.

As the scores highlight, restrictive localization options do not actually increase the speed or scope of data access that Indian law enforcement enjoys. This is because foreign businesses are still required to comply with the laws of their home country while serving consumers in India. This point is especially relevant given the existing market conditions whereby U.S. companies hold most of the world's data and U.S. privacy laws create a significant conflict with Indian laws.

The perceived benefits of data localization for supervisory purposes are therefore a function of local incorporation and authorization requirements. While the Reserve Bank of India has implemented a localization requirement, it is important to note that its localization requirement for payment service providers has been coupled with the fact that the Reserve Bank specifically authorizes these businesses to provide services, a step that requires them to register as Indian businesses.[96] As Indian service providers, such businesses are then regulated primarily by Indian law and the Reserve Bank of India.

Which Localization Measure Would Best Spur Economic Growth?

Many have asserted that localizing the data of Indian consumers within India would likely boost India's economic growth and support innovation more than the free flow of data.[97] While there have been some studies on the impact of localization requirements in India,[98] no study has analyzed costs and benefits of data localization across the economy comprehensively.
This analysis highlights the *relative* efficacy of different localization alternatives instead of providing an absolute quantification of costs and benefits. It analyzes which localization alternative (if any) would benefit Indian producers and the larger economy *more* than the status quo framework of free-flowing data. This analysis looks at how different data localization alternatives fare on four criteria: increasing demand for local goods and services, providing Indian firms a competitive advantage, the countervailing risk of India losing access to data held by foreign companies that opt to pull out of India rather than face greater regulations, and the countervailing risk of foreign governments retaliating against Indian firms abroad.

Of these, the most weight is given to the first two criteria due to their direct relevance to economic growth. Both these criteria receive approximately equal importance (36 and 38 percent, respectively).

Localization has the potential to increase local demand for data storage services, and this is an important factor that the impact of localization measures should be measured against. Similarly, many have argued that localization will be beneficial for India because it would lead to competitive advantages for local industry, and this has become another important reason articulated for requiring localization in India. The countervailing risks of lost businesses (18 percent) and retaliatory action (8 percent) are given slightly higher weights here than they were in the law enforcement case. This is because, by comparison, lost businesses and retaliatory actions by other governments against Indian firms are more likely to have a direct impact on economic performance than on the data-access capabilities of law enforcement. Specific reasons for the relatively low weightage for the countervailing risks have been provided in the previous section. Those reasons remain the same for the purposes of weighting criteria for this objective.

A detailed explanation of these considerations and the findings is given below.

Increased Demand for Goods and Services

This analysis considers whether data localization would increase the demand for data storage services and data storage infrastructure in India. Data storage services in the country are already growing, but it is hard to determine how much of this growth is driven by the anticipation of data localization requirements being imposed.[99] The *relative increase* in demand for such goods and services is therefore assessed depending on the localization measure imposed (see column C1 in appendix 3).

Data localization is likely to spur demand for the establishment of data centers in India. India is one of the largest consumers of data in the world, and the size of its market is likely to double in the next five years.[100] At least some of the demand for storing this data is likely to be met locally, and localization measures can give a fillip to such demand.

Data centers can have significant positive benefits for local economies. A 2014 impact assessment of Facebook's data center in Sweden done by the Boston Consulting Group found significant direct spending in the local area resulting from the establishment of the data center, and the study also estimated that a total of 4,500 jobs would be directly and indirectly created during the life cycle of the center. It also found that the presence of the company and its data center contributed to "the emergence of a new ecosystem of information and communication technology companies . . . public and private investments in infrastructure and utilities."[101]

A report by the U.S. Chamber of Commerce on the benefits of data centers in the United States stated that data centers create close to an average of 1,700 direct and indirect jobs when they are being built and produce $243.5 million in output within a state.[102] Other reports on the impacts of

data centers have noted similar direct and indirect benefits.[103] One report states that data centers contributed to the creation of more than 45,000 jobs in the U.S. state of Virginia in 2018.[104] Another report studying the impact of data centers in the state of Washington estimates that the job multiplier effect of data centers ranges from 2 to 3.54.[105] In other words, for every job created within a data center, there are 2 to 3.54 jobs created in the local economy.

It is likely that the establishment of data centers could have similar potential benefits for the Indian economy. This possibility merits giving a significant weight to the effects that localization requirements may have on the demand for such goods and services in India. In addition, the discussion above highlights that stricter data localization requirements would presumably lead to higher demand for data centers in India.

However, it must be noted that domestic demand could be affected based on the value of imported equipment required for data centers. A recent study by an Indian institution states that, while India has comparative advantages in the production of certain items required for building data centers, in the past few years, imports of equipment for data centers have grown at a much faster rate than exports (with compound annual growth rates of 13.8 percent and 7.4 percent, respectively).[106] In addition, India's overall trade balance has been worsening over the years, and there is very little added domestic value for India on such imported products. So, even though demand for data-related infrastructure can lead to GDP growth, the overall impact on GDP growth would also depend on whether this demand is met with domestic production or imports.

On the whole, while localization measures would likely lead to an increase in demand for data centers and indirect benefits to the economy, the overall effect of such demand on India's GDP could be negated to some extent by the trade imbalance alluded to above. This would be especially true in the short term when the existing trend of increasing trade imbalances would be hard to reverse.

This analysis gives a modest increase in scoring to localization measures that promote the increased usage of local data centers. A stricter localization mandate would result in the highest increase in demand for data storage infrastructure and services because it would provide the highest incentives for increasing local creation and production of data storage infrastructure within India. That likely means hard, unconditional localization would lead to the highest increase in demand (alternative A6 in appendix 3), followed closely by requiring local data storage with global processing (alternative A5 in appendix 3).

The current baseline scenario of mostly unrestricted data flows receives the lowest score (alternative A1), and data mirroring requirements also would likely create very limited additional demand (alternatives A2 and A3) because data would continue to be stored in the most cost-effective loca-

tions for firms and would therefore not necessarily incentivize further creation of data storage infrastructure in India.

Competitive Advantage for Indian Domestic Firms

Mandating data localization in India might put foreign firms at a disadvantage for two reasons. First, these firms would have to incur the costs of data storage and processing capabilities in India as a capital investment. Second, the recurring costs of renting or operating data-related infrastructure in India would be higher than foreign firms' existing costs. Conversely, restricting access to data storage facilities in India may lead to higher prices for such services than at present.[107]

But these consequences would also affect Indian firms that currently store their consumer data outside India.[108] In addition, while some have argued that the storage of Indian data within India would give a boost to domestic innovation, it is unclear how this would work in practice.[109] While the increased availability of data may have some economic benefits,[110] the sharing of proprietary personal data would require additional policy measures, and even if such measures are contemplated, it is unclear if data localization is necessary to implement them. In addition, as mentioned before in the law enforcement section above, data localization does not advance jurisdictional claims for data access. Jurisdictional claims for data access must be advanced by creating licensure or authorization requirements for the operation of the relevant foreign businesses in India, while making data sharing a condition of such authorization.

The earlier discussion on the risk of loss of data in the law-enforcement objective details the issues with automatically assuming that Indian businesses would step in to replace any foreign service providers that may decide not to provide services in India. As previously discussed, in the wake of India's ban on Chinese apps in India in 2020, Indian businesses found it hard to replace successful Chinese apps. While this assumption of substitution by Indian businesses may hold true in the medium to long term, it would be hard to attribute any such substitution solely to data localization, especially over a long time period.

Additionally, barriers to the free flow of data could also hurt Indian businesses by increasing delays and costs in terms of innovation if such businesses have collaborative ties with research or business partners outside India.[111] Indian businesses would also need to use multiple data storage facilities if they serve consumers outside India. Another study finds a positive correlation between innovation and exports of digital services.[112] Lastly, some research implies that additional costs in technologically dynamic sectors seem to lead to greater concentration and further consolidates the market dominance of "superstar firms":

> "Growth of concentration is disproportionately apparent in industries experiencing faster technical change as measured by the growth of patent intensity or total factor productivity, suggesting that technological dynamism, rather than simply anticompetitive forces, is an important driver—though likely not the only one—of this trend."[113]

The costs of localization may therefore be internalized better by large multinational technology firms than Indian ones, negating significant competitive advantages.

Consequently, while local storage requirements, including unconditional hard localization (alternatives A5 and A6 in appendix 3), provide a slight competitive advantage to local firms by forcing foreign firms to invest in data storage services in India, this benefit is not significantly higher than the baseline scenario (alternative A1) because a significant proportion of data center equipment is imported and does not add to Indian GDP. This could, however, change if the growing data center business in India were able to use Indian-manufactured equipment, or if other benefits such as job creation significantly outweighed any loss of benefits. Moreover, these benefits have to be weighed against the other disadvantages discussed above. Mirroring and conditional local storage requirements (alternatives A3, A7, A8, and A9 in appendix 3) also provide some advantages compared to the baseline scenario, but these benefits are lower than local storage alternatives since the costs of these requirements on foreign firms would be lower.

Risk of Data-Holding Foreign Businesses Exiting India

The risk of lost business related to foreign-controlled Indian data could be consequential for India's economy if foreign service providers opt to stop providing existing services or stop innovating for the Indian market in the face of heightened regulations.[114] Businesses may be inhibited from providing data-related services in India due to localization requirements that increase compliance costs, privacy concerns, or both.

The greatest risk arises from conditional hard localization measures (alternative A6 in appendix 3). The risks in that scenario may likely be higher than the risk from an unconditional hard localization measure depending on how critical personal data is defined (alternatives A7, A8, and A9 in appendix 3). If the way the Indian government defines critical personal data raises privacy concerns in jurisdictions like the United States, this could lead to a higher risk of lost business than even an unconditional hard localization measure. Predictably, the lowest risk of lost business related to Indian data emanates from alternatives that impose few or no restrictions on free data flows (alternatives A1–A5 in appendix 3).

Risk of Foreign Retaliation Against Indian Firms Abroad

The countervailing risk of retaliation by foreign governments against Indian firms abroad remains the same under this objective as it was when assessing law enforcement's data access. Stringent localization alternatives carry a higher risk of retaliatory action than others (alternatives A6 and A7 in appendix 3).

The scores were aggregated to understand which alternatives would best meet the stated objective.[115] A regime that requires local data storage but permits global processing best meets the objectives of promoting economic growth (alternative A5 in appendix 3). Following very closely in second are regimes that require mirroring of Indian data within India (alternatives A3 and A4). The hard localization requirement alternative is also a close second-best alternative (alternative A6). If hard localization mandates are adopted, an unconditional localization measure scores higher than conditional localization measures (alternatives A7, A8, and A9). This is because unconditional localization scores higher on the effect it has on stimulating demand for domestic goods and services compared to conditional localization. This means that the localization measure proposed in India's data protection bill is not likely to be the design that can best achieve the government's stated objectives for economic growth and innovation.

Conclusion

Some key findings from the previous two sections bear repetition. Most significantly, access to data stored outside India will require either or both of the following: a regulatory mechanism that would allow India to advance a jurisdictional claim on the entities that store foreign-controlled content data of Indian citizens and bilateral/multilateral agreements that reduce or remove conflicts between Indian law and foreign (especially U.S.) law. Localization does not advance jurisdictional claims or reduce conflicts in jurisdiction.

Ultimately, the best localization alternative for Indian law enforcement purposes is to enter into bilateral agreements with countries that restrict access to such data. Localization measures do not improve access to data significantly with respect to the United States because of domestic U.S. laws, though they may help improve data access with respect to Indian service providers incorporated in other countries. This is because, unlike the United States, many other jurisdictions do not prevent access to personal data of nonresidents stored in their country. Even so, since a large proportion of Indian consumer data is collected and stored by U.S. entities, localization is unlikely to be the best overall strategy for improving law enforcement's data access.

Meanwhile, a localization framework involving local data storage and global processing appears to be the best alternative for enabling higher economic growth in India. This option is closely followed by measures requiring mirroring of data, and alternatively, an unconditional, hard localization requirement. The key driver of these alternatives is the anticipated increase in the demand for goods and services pursuant to forced localization. That fact notwithstanding, India has an increasingly negative trade balance in the trade of equipment for data centers. The degree of impact this would have on India's net GDP growth depends on the continuation of this pattern of trade imbalance.

Notably, localization itself does not ensure data access that would drive innovation in India. Such access is contingent on India exercising legal jurisdiction over entities that collect and control this data, not on the data itself.

These analytical findings are contingent on the stylized design of the localization alternatives and an assessment of existing facts and risks. It is likely that domestic policy measures or geopolitical changes may affect the validity of this analysis. Still, these findings highlight the *relative benefits* of different localization measures in the specific context of a developing country like India. India's 2019 Personal Data Protection Bill imposes a conditional, local storage requirement on personal data. This alternative is not the most beneficial alternative in terms of meeting law enforcement's needs or spurring India's economic growth. The Indian government and other governments around the world can use this framework to balance different considerations while deciding on the feasibility of data localization requirements and other related policies.

Appendix 1: The Theoretical Underpinnings of the Criteria Weighting

Scale of Relative Importance

Score on Scale of Relative Importance	Meaning
1	Equal importance
3	Moderate importance
5	Strong importance
7	Very strong importance
9	Extreme importance
2, 4, 6, 8	Intermediate values
⅓, ⅕, ⅐, ⅑	Values for inverse comparison

SOURCE: Roseanna W. Saaty, "The Analytic Hierarchy Process: What It Is and How It Is Used," *Mathematical Modelling* 9, no. 3–5 (1987): 163, https://core.ac.uk/download/pdf/82000104.pdf.

Saaty's scale allowed the authors to rank the criteria introduced in the methodology section of the paper in relation to each other based on relative importance. Tables 6 and 7 provide the relative comparison matrices for both the objectives: data access for law enforcement and improving economic growth. The example below in table 6 provides a breakdown of how the criterion scope of access was weighted by relative importance compared to the other criteria and itself.

TABLE 6

Analytical Hierarchy Process (Step 1) for Law Enforcement Access to Data Objective

Pairwise Comparison Matrix

Criteria	Scope of Access	Speed of Access	Risk of Retaliation Against Indian Firms Abroad	Risk of Data Loss Due to Foreign Firm Exits
Scope of Access	1	½	5	4
Speed of Access	2	1	7	5
Risk of Retaliation Against Indian Firms Abroad	⅕	⅐	1	⅕
Risk of Data Loss Due to Foreign Firm Exits	¼	⅕	5	1
Sum	**3.45**	**1.842857143**	**18**	**10.2**

By way of example, to fill up the first row of numbers in table 6, the authors answered four questions.

1. How important is scope of access in relation to itself? Here, the criterion was simply measured against itself, giving a value of 1, which signifies equal importance.

2. How important is scope of access to speed of access? Getting access to all types of data is a very important requirement for law enforcement. Yet while law enforcement agencies can usually access metadata and subscriber data easily, they cannot access content data easily. In addition, getting speedy access to data allows law enforcement to determine what other kinds of data are required and seek access to this data too. Therefore, the authors concluded that localization is less of an imperative for scope of access than it is for speed of access. This is why a value of 1/2 was assigned. This value is employed for inverse comparison and shows that scope of access is less important than speed of access.

3. How important is scope of access to the risk of retaliatory action against Indian firms abroad? Scope of data access is significantly more important than the risk of retaliation against Indian firms abroad. This is because the probability of such retaliatory action is low. In addition, these issues were examined from a law enforcement perspective, the gains from access significantly outweigh the risks of retaliation. This is why a value of 5 was assigned, signaling strong relative importance.

4. How important is scope of access in terms of the risk of lost data stemming from foreign firms leaving India? Scope of access is more important to Indian law enforcement than the potential loss of data. While Indian law enforcement will lose access to a foreign firm's data altogether if the firm chooses to leave India, the scope of access is still significantly more important to Indian law enforcement. This is why an intermediate value of 4 was assigned, signaling a strong relative importance for the criterion of scope of data compared to loss of data.

A similar exercise was conducted for all the other criteria in this matrix. But this was just the initial step in the process as the final weighting computation required more steps.

Similarly, below in table 7 is a breakdown of how the criterion demand for goods and services was weighted by relative importance compared to the other criteria and itself.

TABLE 7

Analytical Hierarchy Process (Step 1) for Economic Growth Objective

Pairwise Comparison Matrix

Criteria	Demand for Goods and Services	Competitive Advantage to Domestic Producers/ Competitors	Loss of Data	Risk of Retaliatory Action
Demand for Goods and Services	1.00	1.00	3.00	3.00
Competitive Advantage to Domestic Producers/ Competitors	1.00	1.00	3.00	4.00
Loss of Data	⅓	⅓	1.00	4.00
Risk of Retaliatory Action	⅓	⅓	¼	1.00
Sum	**2.67**	**2.58**	**7.25**	**12.00**

Weighing the criteria for the second objective (spurring economic growth) entailed conducting the same exercise again (see table 7) by answering the following four questions.

1. How important is demand for goods and services in relation to itself? Here, the criterion is simply measured against itself, giving a value of 1, which signifies equal importance.

2. How important is demand for goods and services in relation to a boost to Indian firms' competitive advantage? Competitive advantage is equally important to demand for goods and services because, while competitive advantage for domestic producers is important from the government's perspective, the demand created is equally important. This is why it is assigned a value of 1, signifying equal importance.

3. How important is demand for goods and services in terms of the risk of lost data stemming from foreign firms leaving India? Demand for goods and services is slightly more important than the risk of data loss. The risk of loss of data has low impact on economic growth and innovation because data is nonrival and can be recollected/generated. In addition, the actual probability of the risk materializing is low based on existing evidence of the behavior of foreign firms and investments coming into India. Compared to this, the benefits from heightened demand for goods and services is of larger economic importance to India's domestic economy. This is why it was assigned a value of 3, signaling moderate importance.

4. How important is demand for goods and services in relation to the risk of foreign retaliation against Indian firms abroad? Admittedly, the risk of such retaliation would also affect Indian firms operating abroad and thus directly impact India's economic growth. But heightened demand for goods and services is still more important for India's economy than the risk of foreign retaliation. This is why it has been assigned a value of 3 signaling moderate importance.

Again, a similar exercise was conducted for all the other criteria in this matrix. But this was just the initial step in the process as the final weighting computation required more steps.

Appendix 2: Measuring Law Enforcement Data Access and Data Localization

Alternatives	**Criteria**				
	Scope of Access (Weight: 31/100) (C1)	**Speed of Access** (Weight: 50/100) (C2)	**Risk of Retaliation Against Indian Firms** (Weight: 05/100) (C3)	**Risk of Data Loss** (Weight: 14/100) (C4)	**Score** (S=C1+C2+C3+C4)
No localization (global storage and processing of data with MLATs) **(A1: Baseline)**	6*31=186	3*50=150	9*5=45	9*14=126	**507**
Rationale	*1.1. Scope of Access:* Moderate (baseline).	*1.2. Speed of Access:* Low. Law enforcement can request that foreign firms grant access to data that they do not have jurisdiction over by going through an MLAT process. On average, such requests take ten months before data access is granted.	*1.3. Risk of Retaliation Against Indian Firms:* Lowest risk of retaliatory action because there would be minimal reason for retaliatory action against Indian firms if the Indian government keeps permitting the global storage and global processing of data.	*1.4. Risk of Data Loss:* The risk of data loss due to foreign firms choosing to leave or not to enter India due to localization requirements would be lowest in this alternative with no additional localization requirements.	
No localization (global storage and processing of data with bilateral/ multilateral agreements for data access) **(A2)**	9*31=279	9*50=450	9*5=45	9*14=126	**900**
Rationale	*2.1. Scope of Access:* Significantly higher than the baseline. This is because bilateral and multilateral agreements would allow law enforcement to access a larger amount of data that is the subject of the agreement(s).v	*2.2. Speed of Access:* Significantly higher than the baseline. This is because Indian law enforcement would be able to access data of all firms with which India has a bilateral or a multilateral agreement.	*2.3. Risk of Retaliation Against Indian Firms:* This alternative would again pose the lowest risk of retaliatory action to Indian firms abroad as no additional stringent localization measures would be adopted.	*2.4. Risk of Data Loss:* The risk of data loss due to foreign firms choosing to leave or not enter India due to localization requirements would continue to be as low in this alternative as in the previous one for the same reason.	

Alternatives	Criteria				
	Scope of Access (Weight: 31/100) (C1)	**Speed of Access** (Weight: 50/100) (C2)	**Risk of Retaliation Against Indian Firms** (Weight: 05/100) (C3)	**Risk of Data Loss** (Weight: 14/100) (C4)	**Score** (S=C1+C2+C3+C4)
Free flow of data with mirroring (with MLATs) **(A3)**	6*31=186	3*50=150	8*5=40	8*14=112	**488**
Rationale	*3.1. Scope of Access:* Moderate (same as the baseline).	*3.2. Speed of Access:* Low (same as the baseline).	*3.3. Risk of Retaliation Against Indian Firms:* Slightly higher risk than no localization because of the imposition of a localization requirement in the form of mirroring. Mirroring may not entail a significantly higher risk.	*3.4. Risk of Data Loss:* The risk of data loss due to firms choosing to leave or not enter India due to localization requirements would be slightly higher in this alternative than in the previous one. This is because mirroring does not impose significant local storage requirements, nor does it seriously inhibit global flows of data, though it does increase costs for foreign businesses.	
Free flow of data with mirroring (with bilateral/ multilateral frameworks) **(A4)**	9*31=279	9*50=450	8*5=40	8*14=112	**881**
Rationale	*4.1. Scope of Access:* Same as no localization with multilateral/bilateral frameworks (A2).	*4.2. Speed of Access:* Same as no localization with multilateral/bilateral frameworks.	*4.3. Risk of Retaliation Against Indian Firms:* Same as A3.	*4.4. Risk of Data Loss:* The risk of data loss due to foreign firms choosing to leave or not enter India due to localization requirements would be the same as in A3. This is because mirroring does not impose significant local storage requirements, nor does it seriously inhibit global flows of data, though it does increase costs for foreign businesses.	

Alternatives	Criteria				
	Scope of Access (Weight: 31/100) (C1)	**Speed of Access** (Weight: 50/100) (C2)	**Risk of Retaliation Against Indian Firms** (Weight: 05/100) (C3)	**Risk of Data Loss** (Weight: 14/100) (C4)	**Score** (S=C1+C2+C3+C4)
Local storage with global processing (A5)	7.5*31=232.5	6*50=300	5*5=25	6*14=84	**641.5**
Rationale	*5.1. Scope of Access:* In this alternative, while the data would be locally stored, Indian law enforcement would still not be able to access content data due to U.S. law, though it would gain access to non-U.S.-controlled foreign data.	*5.2. Speed of Access:* Moderate. This is because while all data may be stored in India, Indian law enforcement still would not be able to easily access it due to U.S. laws that prohibit U.S. companies from providing such data. Data collected by non-U.S. companies could potentially be accessed more quickly than in the baseline.	*5.3. Risk of Retaliation Against Indian Firms:* There would be a higher risk in this case than in the previous alternative. That is because this alternative would pose serious constraints on the movement of data outside the country. This requirement also would prevent Indian data from being stored in the countries where service-providing businesses may be incorporated and whose laws they may be subject to (like the United States). This would heighten the risk of retaliatory action significantly in this scenario compared to previous alternatives.	*5.4. Risk of Data Loss:* Higher risk of data loss due to higher costs of localization-related compliance and higher concerns about privacy in foreign jurisdictions.	
Hard localization (A6)	7.5*31=232.5	6*50=300	2*5=10	4*14=56	**598.5**
Rationale	*6.1. Scope of Access:* Same as local storage, global processing (A5).	*6.2. Speed of Access:* Same as local storage, global processing (A5).	*6.3. Risk of Retaliation Against Indian Firms:* This alternative would pose the highest risk of retaliatory action to Indian firms abroad since all data would have to stay in India.	*6.4. Risk of Data Loss:* Foreign businesses would face higher costs compared to those under the previous alternative, likely leading to a higher possibility of foreign businesses deciding not to provide services in India compared to A5.	

Alternatives	Criteria				
	Scope of Access (Weight: 31/100) (C1)	**Speed of Access** (Weight: 50/100) (C2)	**Risk of Retaliation Against Indian Firms** (Weight: 05/100) (C3)	**Risk of Data Loss** (Weight: 14/100) (C4)	**Score** (S=C1+C2+C3+C4)
Conditional hard localization	6.5*31=201.5	6*50=300	4*5=20	3*14=42	**563.5**
(A7)					
Rationale	*7.1. Scope of Access:* Lower in this alternative compared to the previous alternative. This is because, while Indian law enforcement personnel would get access to some data stored in the EU, they still would not get access to data stored in the United States. The scope of access in this scenario could be further reduced, depending on the definition of critical personal data. This scenario, however, would still offer higher data access than the baseline scenario.	*7.2. Speed of Access:* Same as local storage, global processing (A5).	*7.3. Risk of Retaliation Against Indian Firms:* Slightly lower than A6. Even though less data would be localized under this scenario, one of the sources of risk in this case would be the privacy-related activism of foreign governments. Therefore, even if the economic reasons for taking retaliatory action would be reduced, the risk of privacy-related actions would remain.	*7.4. Risk of Data Loss:* On the one hand, there may be slightly lower direct costs of conditional localization under this scenario compared to hard localization. On the other hand, the privacy-related negative effects (such as bad publicity and shareholder activism) could be higher if only critical personal data is localized. This would also depend on how critical personal data is defined with sensitivity to privacy issues being higher if critical personal data can be targeted for government misuse. Therefore, on balance, the privacy-related negative effects would be slightly higher in this scenario than in the preceding alternatives, so the overall score here would be slightly lower than all the preceding alternatives.	

Alternatives	Criteria				
	Scope of Access (Weight: 31/100) (C1)	**Speed of Access** (Weight: 50/100) (C2)	**Risk of Retaliation Against Indian Firms** (Weight: 05/100) (C3)	**Risk of Data Loss** (Weight: 14/100) (C4)	**Score** (S=C1+C2+C3+C4)
Conditional soft localization **(A8)**	6.5*31=201.5	6*50=300	5*5=25	3*14=42	**568.5**
Rationale	*8.1. Scope of Access:* Same as A7. Lower in this alternative compared to A6 above. The scope of data access here would, however, still be higher compared to the baseline scenario (since data stored by EU businesses in the EU would be available to Indian law enforcement). This is why a value of 6.5 of 10 was given.	*8.2. Speed of Access:* Same as A5.	*8.3. Risk of Retaliation Against Indian Firms:* Same as A5.	*8.4. Risk of Data Loss:* Same as A7, since higher weight was accorded to privacy-related negative consequences of localizing data.	
Conditional mirroring **(A9)**	6.5*31=201.5	6*50=300	8*5=40	3*14=42	**583.5**
Rationale	*9.1. Scope of Access:* Same as A8. This scope will, however, still be higher compared to the baseline scenario.	*9.2. Speed of Access:* Same as A5.	*9.3. Risk of Retaliation Against Indian Firms:* Same as A3.	*9.4. Risk of Data Loss:* Same as A7, since higher weight was accorded to privacy-related negative consequences of localizing data.	

Assumption 1: If India enters into a bilateral/multilateral agreement, it will be more beneficial for data access than the current system of seeking information through an MLAT. For details regarding this assumption, see appendix 2. Assumption 2: Critical personal data is a smaller set of personal data than sensitive personal data.

Appendix 3: Measuring Boosted Economic Growth and Data Localization

Alternatives	**Criteria**				
	Demand for Goods and Services (Weight: 36/100) (C1)	**Competitive Advantage for Domestic Producers** (Weight: 38/100) (C2)	**Risk of Retaliation Against Indian Firms** (Weight: 8/100) (C3)	**Risk of Lost Data Business** (Weight: 18/100) ;(C4)	**Score** (S=C1+C2+C3+C4)
No localization (Global storage and processing of data with MLATs) **(A1: Baseline)**	0*36=0	2*38=76	9*8=72	9*18=162	**310**
Rationale	*1.1. Demand for Goods and Services:* This analysis highlights both direct and indirect demand for goods and services in light of anticipated localization requirements. Direct demand for goods and services would take the form of infrastructure requirements and demand for labor. Indirect demand would take the form of demand for complementary services, local infrastructure, and facilities for employees. The building of data centers is also likely to lead to increases in tax revenues, which are a net addition to GDP even though they do not increase demand for goods and services. Yet net demand for goods and services will depend on the extent to which such goods and services are sourced from within India. If the goods are imported, such demand will add to the GDP of other countries and not India's. A recent Indian study shows that India is a net importer of equipment required for data centers and that the negative trade balance has been increasing over time. In this status quo scenario, no additional demand for infrastructure for local storage attributable to localization policies would be created. Demand would be driven by other market pressures and policy measures.	*1.2. Competitive Advantage for Domestic Producers:* In this baseline alternative, foreign companies can operate in India while not having any additional mandated local costs in terms of storing or processing data in most sectors. Domestic Indian firms so far do not seem to enjoy significant benefits compared to foreign firms.	*1.3. Risk of Retaliation Against Indian Firms:* This alternative would pose the lowest risk of foreign retaliation against Indian firms abroad.	*1.4. Risk of Lost Data Business:* The risk of data loss due to firms choosing to leave or not enter India due to localization requirements would be lowest in this alternative.	

Alternatives	Criteria				
	Demand for Goods and Services (Weight: 36/100) (C1)	**Competitive Advantage for Domestic Producers** (Weight: 38/100) (C2)	**Risk of Retaliation Against Indian Firms** (Weight: 8/100) (C3)	**Risk of Lost Data Business** (Weight: 18/100) ;(C4)	**Score** (S=C1+C2+C3+C4)
No localization (Global storage and processing of data with bilateral/ multilateral agreements for data access) **(A2)**	3*36=108	2*38=76	9*8=72	9*18=162	**418**
Rationale	*2.1. Demand for Goods and Services:* In this alternative, localization measures would go into effect only with respect to countries with which India does not have any bilateral or multilateral agreements. This arrangement would lead to some demand for infrastructure requirements from firms operating out of jurisdictions without any bilateral agreements. However, this demand could also be negated if such firms choose to shift operations to countries with bilateral agreements. They would do so in order to continue providing services to Indian consumers but may find it preferable to store data outside India. In addition, a significant portion of the additional demand would be met through imports unless existing domestic capacity is ramped up	*2.2. Competitive Advantage for Domestic Producers:* Foreign firms that want to process Indian data would either have to locally store and process data or do so in a country with which India has a bilateral/multilateral framework. So the cost for foreign companies may be higher in this alternative than the previous alternative, depending on the cost of storage in India and participating countries. The critical condition is the cost of data storage in India. These advantages have to be weighed against the disadvantages to Indian firms that currently store data outside India but would have to either switch to a country with which India has signed an agreement or move back to India after this framework is in place. The competitive advantage for local firms could actually remain the same as the previous alternative.	*2.3. Risk of Retaliation Against Indian Firms:* This alternative would again pose the lowest risk of foreign retaliation against Indian firms abroad as no stringent localization measures would be adopted.	*2.4. Risk of Lost Data Business:* The risk of data loss due to firms choosing to leave or not enter India due to localization requirements would continue to be as low in this alternative as in the previous one.	

Alternatives	Criteria				
	Demand for Goods and Services (Weight: 36/100) (C1)	**Competitive Advantage for Domestic Producers** (Weight: 38/100) (C2)	**Risk of Retaliation Against Indian Firms** (Weight: 8/100) (C3)	**Risk of Lost Data Business** (Weight: 18/100) ;(C4)	**Score** (S=C1+C2+C3+C4)
Free flow of data with mirroring (with MLATs) **(A3)**	3*36=108	2.5*38=95	8*8=64	9*18=162	**429**
Rationale	*3.1. Demand for Goods and Services:* Mirroring requires less infrastructural capacity and investment than local storage. There would be higher demand for infrastructure for local storage under this scenario than with the no localization option, but demand would be lower than it would be with local storage requirements. However, because data would be allowed to flow freely and be stored anywhere around the world, the increased demand for goods and services attributable to localization would not be significantly higher.	*3.2. Competitive Advantage for Domestic Producers:* Any competitive advantage for Indian firms would be minimal because the status quo would stay mostly the same, as mirroring is not a significant expense.	*3.3. Risk of Retaliation Against Indian Firms:* Slightly higher risk than in the scenario involving no localization. Mirroring may not entail a significantly higher risk.	*3.4. Risk of Lost Data Business:* The risk of data loss due to firms choosing to leave or not enter India due to localization requirements would be slightly higher in this alternative compared to the previous one. This is because mirroring does not impose significant local storage requirements, nor does it seriously inhibit global flows of data, but it does increase costs for foreign businesses.	
Free flow of data with mirroring (with bilateral/ multilateral frameworks) **(A4)**	3.5*36=126	2*38=76	8*8=64	9*18=162	**428**
Rationale	*4.1. Demand for Goods and Services:* In this alternative, there would be additional demand for local storage since storage requirements would be limited by bilateral or multilateral agreements. There could also be some demand for infrastructure requirements from firms operating out of jurisdictions without any bilateral/multilateral agreements. However, a significant portion of the additional demand would be met through imports unless existing domestic capacity were ramped up.	*4.2. Competitive Advantage for Domestic Producers:* Same as under the scenario involving no localization with multilateral/bilateral agreements. The cost of mirroring continues to be an insignificant expense.	*4.3. Risk of Retaliation Against Indian Firms:* Same as A3.	*4.4. Risk of Lost Data Business:* The risk of data loss due to firms choosing to leave or not enter India due to localization requirements would slightly higher in this alternative compared with the previous one. This is because mirroring does not impose significant local storage requirements, nor does it seriously inhibit global flows of data, but it does increase costs for foreign businesses.	

Alternatives	Criteria				
	Demand for Goods and Services (Weight: 36/100) (C1)	**Competitive Advantage for Domestic Producers** (Weight: 38/100) (C2)	**Risk of Retaliation Against Indian Firms** (Weight: 8/100) (C3)	**Risk of Lost Data Business** (Weight: 18/100) ;(C4)	**Score** (S=C1+C2+C3+C4)
Local storage with global processing (A5)	5*36=180	3*38=114	5*8=40	6*18=108	**442**
Rationale	*5.1. Demand for Goods and Services:* This alternative would include a significantly higher demand for infrastructure for local storage (compared to all previous alternatives). This is because this alternative would mandate that all data be locally stored. However, since data could still be processed abroad, the direct and indirect demand for human capital would be lower compared to alternatives where local processing is mandated. In addition, some of the benefits may, however, be offset by lower demand resulting from higher costs of local storage and processing and the negative effects on trade. Imports of goods required for data centers would be highest under local storage requirement alternatives.	*5.2. Competitive Advantage for Domestic Producers:* Foreign firms would have a switching cost due to local storage requirements. However, some Indian companies may also have a switching cost, negating their advantage over their foreign competitors. The advantage would be highest for those who already store data within India. These local companies would have some competitive advantage because of the lack of switching costs and the initially higher operating costs. This, however, would be a one-time cost/benefit and would be unlikely to recur.	Risk of Retaliation Against Indian Firms: There would be a higher risk of retaliation in this scenario compared to the previous alternative. In this case, serious constraints on the movement of data would be imposed. This requirement also would prevent Indian data from being stored in countries in which service- providing businesses may be incorporated and whose laws they may be subject to (like the United States). This scenario therefore heightens the risk of retaliation significantly compared to previous alternatives.	5.4. Risk of Lost Data Business: In this case, the risk of data loss would be greater due to higher costs of localization-related compliance and larger concerns about privacy in foreign jurisdictions.	
Hard localization (A6)	6*36=216	3*38=114	2*8=16	4*18=72	**418**
Rationale	*6.1. Demand for Goods and Services:* This alternative would likely see the highest demand for infrastructure. There likely would be slightly higher demand for data processing activities within India compared to the previous alternative. This is because all data would need to be stored and processed within India. This may, however, be offset by lower demand resulting from higher costs of local storage and processing and the negative effect on trade.	*6.2. Competitive Advantage for Domestic Producers:* Same as A5, since there would be no additional direct costs for foreign firms.	*6.3. Risk of Retaliation Against Indian Firms:* This alternative would see the highest risk of retaliation against Indian firms abroad since all data must stay in India.	*6.4. Risk of Lost Data Business:* Higher costs would be faced by businesses compared to the previous alternative, likely leading to a higher possibility of businesses deciding not to provide services in India compared to A5.	

Alternatives	Criteria				
	Demand for Goods and Services (Weight: 36/100) (C1)	**Competitive Advantage for Domestic Producers** (Weight: 38/100) (C2)	**Risk of Retaliation Against Indian Firms** (Weight: 8/100) (C3)	**Risk of Lost Data Business** (Weight: 18/100) ;(C4)	**Score** (S=C1+C2+C3+C4)
Conditional hard localization **(A7)**	5.5*36=198	2.5*38=95	3*8=24	3*18=54	**371**
Rationale	*7.1. Demand for Goods and Services:* This alternative would prompt lower demand for infrastructure than the previous alternative. There might be slightly higher demand for data processing activities within India for activities related to sensitive and critical personal data. The bulk of data would be allowed to flow out of India. The demand for goods and services would therefore be lower than in the unconditional local storage alternatives.	*7.2. Competitive Advantage for Domestic Producers:* The competitive advantage would be slightly reduced in this scenario compared to hard localization because switching costs may vary marginally depending on the amount of data required to be stored.	*7.3. Risk of Retaliation Against Indian Firms:* Slightly lower than A6. Even though less data would be localized in this case, one of the sources of risk in this criterion is the privacy-related activism of foreign governments. Therefore, even if the economic reasons for retaliating would be less pronounced, the risk of privacy-related actions would remain.	*7.4. Risk of Lost Data Business:* On one hand, there may be slightly lower direct costs of conditional localization compared to hard localization. On the other hand, the privacy-related negative effects (such as bad publicity and shareholder activism) could be higher if only critical personal data is localized. This would also depend on how critical personal data is defined (as there may be higher sensitivity to privacy issues if critical personal data is defined to include data that could result in serious privacy violations). Therefore, on balance, the privacy-related negative effects would be slightly higher than in the preceding alternatives. Consequently, the overall score for this alternative would be slightly lower than all the preceding alternatives.	

Alternatives	Criteria				
	Demand for Goods and Services (Weight: 36/100) (C1)	**Competitive Advantage for Domestic Producers** (Weight: 38/100) (C2)	**Risk of Retaliation Against Indian Firms** (Weight: 8/100) (C3)	**Risk of Lost Data Business** (Weight: 18/100) ;(C4)	**Score** (S=C1+C2+C3+C4)
Conditional soft localization **(A8)**	5*36=180	2.5*38=95	5*8=40	3*18=54	**369**
Rationale	*8.1. Demand for Goods and Services:* Demand would be lower than in the previous alternative, since data would be allowed to flow outside India for processing.	*8.2. Competitive Advantage for Domestic Producers:* Same as A7.	*8.3. Risk of Retaliation Against Indian Firms:* Same as A5.	*8.4. Risk of Lost Data Business:* Same as A7.	
Conditional mirroring **(A9)**	3*36=108	2.5*38=95	8*8=64	3*18=54	**321**
Rationale	*9.1. Demands for Goods and Services:* Same as A3.	*9.2. Competitive Advantage for Domestic Producers:* Same as A3.	*9.3. Risk of Retaliation Against Indian Firms:* Same as A3.	*9.4. Risk of Lost Data Business:* Same as A7.	

About the Authors

Anirudh Burman is an associate fellow at Carnegie India.

Upasana Sharma is a research assistant at Carnegie India.

Acknowledgments

The authors are grateful to Rudra Chaudhuri, Suyash Rai, Srinath Raghavan, Rajesh Bansal, Tarunima Prabhakar, and Smriti Parsheera for their help and input. The authors are also grateful to discussants and participants at various forums, including Carnegie India's 2020 Global Technology Summit, who provided valuable comments and feedback on this research. The authors also thank the funders who support Carnegie India's Technology and Society program and would especially like to acknowledge the useful inputs provided by Google India.[116] The views expressed in this piece are solely those of the authors.

Notes

1 Committee of Experts Under the Chairmanship of Justice B. N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (New Delhi: Indian Ministry of Electronics and Information Technology, 2018), https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf.

2 Srikrishna Committee of Experts, "Draft Personal Data Protection Bill, 2018," 2018, https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.

3 Lok Sabha, "The Personal Data Protection Bill, 2019," Bill No. 373 of 2019, 2019, http://164.100.47.4/billsTexts/LSbillTexts/Asintroduced/373_2019_LS_Eng.pdf.

4 For instance, see "Draft National E-Commerce Policy Report: India's Data for India's Development," Indian Ministry of Commerce and Industry Department for Promotion of Industry and Internal Trade, February 23, 2019, https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf; and "Discussion Paper on National Strategy for Artificial Intelligence," Niti Aayog, 2019, https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf.

5 For some examples, see Matthias Bauer, Martina F. Ferracane, and Erik van der Marel, "Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization," Global Commission on Internet Governance Paper Series no. 30, May 2016, https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf.; Rajat Kathuria, Mansi Kedia, Gangesh Varma, and Kaushambi Bagchi, *Economic Implications of Cross-Border Data Flows* (New Delhi: Indian Council for Research on International Economic Relations, November 2019), https://icrier.org/pdf/Economic_Implications_of_Cross-Border_Data_Flows.pdf.; Leviathan Security Group, "Quantifying the Cost of Forced Localization," 2015, https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf; and, Bhaskar Marg and Bani Park, "Data Localisation: India's Double-Edged Sword?" (Jaipur, CUTS International, 2020), https://cuts-ccier.org/pdf/data-localisation-indias-double-edged-sword.pdf.

6 United Nations Conference on Trade and Development (UNCTAD), *Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries* (Switzerland: UNCTAD, 2019), 9, https://unctad.org/en/PublicationsLibrary/der2019_en.pdf.

7 Ibid.

8 Ibid, 41.

9 For a definition of data localization, see Anupam Chander and Uyen P. Le, "Breaking the Web: Data Localization vs. the Global Internet," *Emory Law Journal*, forthcoming UC Davis Legal Studies Research Paper No. 378, April 2014, 3, https://ssrn.com/abstract=2407858. In the introduction, the authors define data localization measures "as those that specifically encumber the transfer of data across national borders."

10 See articles 44 and 45 of the EU's GDPR legislation. European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/ EC (General Data Protection Regulation)," 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

11 Yuxi Wei, "Chinese Data Localization Law: Comprehensive but Ambiguous" University of Washington Henry M. Jackson School of International Studies, February 7, 2018, https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/.

12 "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)," Russian Federal Service for Supervision of Communications, Information Technology, and Mass Media, July 21, 2014, https://pd.rkn.gov.ru/authority/p146/p191/.

13 "Regulation of the Government of the Republic of Indonesia Number 82 of 2012 Concerning Electronic System and Transaction Operation," Office of the President of Indonesia, 2012, https://media2.mofo.com/documents/indonesia+government+regulation+no.+82+of+2012.pdf.

14 Rogier Creemers, Paul Triolo, and Graham Webster, "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," New America, June 29, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

15 Wei, "Chinese Data Localization Law: Comprehensive but Ambiguous."

16 "Regulation of the Government of the Republic of Indonesia Number 82 of 2012 Concerning Electronic System and Transaction Operation."

17 "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)."

18 "My Health Records Act 2012," Australian Federal Register of Legislation, https://www.legislation.gov.au/Details/C2019C00337.

19 In 2018, an amendment to the *My Health Records Act 2012* restricted the ability of the My Health Record system operator to disclose personal information to law enforcement and government agencies without a judicial order or a patient's consent. See "My Health Records Amendment (Strengthening Privacy) Bill, 2018," Australian Parliament, 2018, https://www.aph.gov.au/Parliamentary_Business/bills_LEGislation/bills_Search_Results/Result?bId=r6169.

20 "Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018)," *Federal Register*, August 26, 2015, https://www.federalregister.gov/documents/2015/08/26/2015-20870/defense-federal-acquisition-regulation-supplement-network-penetration-reporting-and-contracting-for#sectno-reference-239.7602-2%20.

21 "EU Data Protection Rules," European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en.

22 *Clarifying Lawful Overseas Use of Data (CLOUD) Act*, H.R. 1625 (115th Congress), 2018, https://epic.org/privacy/cloud-act/cloud-act-text.pdf.

23 Ibid, Section 102.

24 "Osaka Declaration on Digital Economy," Japanese Ministry of Economy, Trade and Industry, June 2019, https://www.meti.go.jp/press/2019/06/20190628001/20190628001_01.pdf.

25 Ibid.

26 "APEC CBPR & PRP: Questions and Answers," Centre for Information Policy Leadership, March 2020, 1, https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/03/cipl_cbpr_and_prp_q_a_final__19_march_2020_.pdf.

27 See Article 19.11 and 19.12 of the United States-Mexico-Canada Agreement. "United States-Mexico-Canada Agreement: Chapter 19," Office of the U.S. Trade Representative, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf.

28 See Article 14.13 of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership. "Consolidated TPP Text: Chapter 14 – Electronic Commerce," Government of Canada, https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/tpp-ptp/text-texte/14.aspx?lang=eng

29 "Australia-Singapore Digital Economy Agreement: Summary of Key Outcomes," Australian Department of Foreign Affairs and Trade, December, 8, 2020, https://www.dfat.gov.au/sites/default/files/australia-singapore-digital-economy-agreement-summary-key-outcomes.pdf.
30 "Storage of Payment System Data," Reserve Bank of India, June 26, 2019, https://m.rbi.org.in/Scripts/FAQView.aspx?Id=130.
31 Arindrajit Basu, Elonnai Hickok, and Aditya Singh Chawla, "The Localization Gambit: Unpacking Policy Measures for Sovereign Control of Data in India," Centre for Internet and Society, March 19, 2019, 21, https://cis-india.org/internet-governance/resources/the-localization-gambit.pdf.
32 "The Public Records Act, 1993," National Archives of India, 1993, http://nationalarchives.nic.in/content/public-records-act-1993-0.
33 See Section 4 of The Public Records Act, 1993.
34 "The Information Technology (IT) Act, 2000," Indian Ministry of Electronics and Information Technology, 2000, https://www.meity.gov.in/content/information-technology-act-2000.
35 Rishab Bailey and Smriti Parsheera, "Data Localization in India: Questioning the Means and Ends," National Institute of Public Finance and Policy, Paper no. 242, October 31, 2018, 9, https://www.nipfp.org.in/media/medialibrary/2018/10/WP_2018_242.pdf.
36 Basu, Hickok, and Chawla, "The Localization Gambit," 21.
37 "National Data Sharing and Accessibility Policy," Indian Ministry of Science and Technology, 2012, https://dst.gov.in/national-data-sharing-and-accessibility-policy-0.
38 Bailey and Parsheera, "Data Localization in India," 8.
39 Ibid.
40 Ibid, 8–9.
41 "Audit Criteria for Cloud Service Providers," Indian Ministry of Electronics and Information Technology, December 2016, https://meity.gov.in/writereaddata/files/CSP-01-03%20-%20Audit%20Criteria%20for%20CSPs.pdf.
42 "National Telecom M2M Roadmap," Indian Ministry of Communications and Information Technology Department of Telecommunications, May 2015, https://dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf.
43 Ibid.
44 "Consolidated FDI Policy," Indian Ministry of Commerce and Industry Department of Industrial Policy and Promotion, August 28, 2017, https://dipp.gov.in/sites/default/files/CFPC_2017_FINAL_RELEASED_28.8.17_1.pdf.
45 See Clause 1.3 (ix) of Annexure 7 of the Consolidated FDI Policy.
46 "IRDAI (Outsourcing of Activities by Indian Insurers) Regulations," Insurance Regulatory and Development Authority, 2017, https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx?page=PageNo3149&flag=1.
47 Reserve Bank of India, "Storage of Payment System Data." Also see paragraph 6.4.9 of the "Oversight Framework for Financial Market Infrastructures (FMIs) and Retail Payment Systems (RPSs)" Reserve Bank of India, 2020, 34 https://www.rbi.org.in/scripts/bs_viewcontent.aspx?Id=3864.
48 Srikrishna Committee of Experts, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, 88. There, the authors note: "It is easier for law enforcement agencies to access information within their jurisdiction as compared to awaiting responses to requests made to foreign entities which store data abroad" and "The question of local storage of personal data is intrinsically connected to the enforcement of domestic law generally and in particular, the data protection law itself."
49 Ibid. The authors also note, "It is important for the law to acknowledge the importance of quick and easy access to information to effectively secure national security and public safety."

50 Timothy Mclaughlin, "How Whatsapp Fuels Fake News And Violence In India," *Wired*, December 12, 2018, https://www. wired.com/story/how-whatsapp-fuels-fake-news-and-violence-in-india; and "Centre Warns Whatsapp Over Abuse of Platform," *Business Standard*, July 4, 2018, https://www.business-standard.com/article/news-ani/centre-warns-whatsapp-over-abuse-of-platform-118070400083_1.html.

51 Niti Aayog, "Discussion Paper on National Strategy for Artificial Intelligence," 79. The authors note, "The proposed data exchange marketplace will attract data providers and model builders / trainers to build AI products. The process of exchange, with enforced provisions of privacy and anonymisation, brings a market determined value to data and thus forces the existing informal data exchange economy, without any privacy protection, to move towards a formal economy. The government can establish a committee of experts, researchers, AI developers and regulators to create the standards the data marketplace will adhere by and explore how can it be put in implementation." Also see Srikrishna Committee of Experts, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, 10. The text reads, "Keeping citizens' personal data protected while unlocking the digital economy, as the TOR mandates, are both necessary. This will protect individual autonomy and privacy which can be achieved within the rubric of a free and fair digital economy. This is the normative framework that India, as a developing nation needs to assuredly chart its course in the increasingly digital 21st century."

52 Srikrishna Committee of Experts, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, 92–93. The authors note, "One of India's key interests with regard to personal data which is critical to India's national security interests and imperative for the smooth running of the wheels of the Indian economy is the prevention of foreign surveillance." They go on to say, "If data is exclusively processed in India, it will potentially cut off foreign surveillance of large amounts of such data. . . . Thus, for the prevention of foreign surveillance critical personal data should be exclusively processed within the territory of India."

53 "Draft National E-Commerce Policy Report: India's Data for India's Development," Indian Ministry of Commerce and Industry Department for Promotion of Industry and Internal Trade, 8. The document notes, "The increasing importance of data warrants treating it at par with other resources on which a country would have sovereign right. It is said that data is the new oil. Therefore, just like oil or any other natural resource, it is important to protect data, prevent its misuse, regulate the use and processing of data and address the concerns related to privacy and security."

54 Kathuria, Kedia, Varma, and Bagchi, *Economic Implications of Cross-Border Data Flows*, 12.

55 *The Global Risks Report 2019*, 14th edition, World Economic Forum, 2019, 16, http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.

56 *The Global Risks Report 2020*, 15th edition, World Economic Forum, 2020, 62, http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.

57 Srikrishna Committee of Experts, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, 13–14.

58 See Srikrishna Committee of Experts, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, 88. The authors note, "The question of local storage of personal data is intrinsically connected to the enforcement of domestic law generally and in particular, the data protection law itself. Intelligence agencies and law enforcement bodies have an increasingly challenging role in the 21st century. They must check the growth of terrorism, prevent cyber-attacks and tackle cyber-crime. Investigation of ordinary crime too often requires access to personal data. Further, the obligations on data fiduciaries pursuant to the data protection framework themselves require effective enforcement by the DPA."

59 Abbas Mardani, Ahmad Jusoh, Khalil MD Nor, Zainab Khalifah, Norhayati Zakwan and Alireza Valipour, "Multiple Criteria Decision-Making Techniques and Their Applications: A Review of the Literature From 2000 to 2014," *Economic Research Ekonomska Istraživanja* 28, no. 1 (2015): https://doi.org/10.1080/1331677X.2015.1075139; Mark Velasquez and Patrick T. Hester, "An Analysis of Multi-Criteria Decision Making Methods," *International Journal of Operations Research* 10, no. 2, 56–66, (2013): http://www.orstw.org.tw/ijor/vol10no2/ijor_vol10_no2_p56_p66.pdf. See Velasquez and Hester, 59. and Gwo-Hshiung Tzeng, Cheng-Wei Lin, and Serafim Opricovic, "Multi-Criteria Analysis of Alternative-Fuel Buses for Public Transportation," *Energy Policy* 33, no. 11 (2005): 1373–1383, https://ir.nctu.edu.tw/bitstream/11536/13527/1/000228628100002.pdf. In particular, Velasquez and Hester highlight "AHP's ability to handle larger problems makes it ideal to handle problems that compare performance among alternatives."

60 The Indian government requires the localization of all government data stored on the cloud. "Cloud Security Best Practices," Indian Ministry of Electronics and Information Technology, 2020, 9–10, https://www.meity.gov.in/writereaddata/files/WI3_Cloud%20Security%20Best%20Practices_06112020.pdf; and "Guidelines for Procurement of Cloud Services," Indian Ministry of Electronics and Information Technology, 2020, 19, 40 https://www.meity.gov.in/writereaddata/files/Guidelines_Procurement_Cloud%20Services_v2.2.pdf. Moreover, India's omnibus information technology law—the Information Technology Act, 2000—was amended to implement India's National Cyber Security Policy of 2013. These amendments allow for enhanced security requirements for India's "critical information infrastructure," which covers government agencies and departments in various sectors such as power, IT, finance and banking, transportation, and e-governance. See Saikat Datta, "The NCIIPC and Its Evolving Framework," Observer Research Foundation, November 3, 2016, https://www.orfonline.org/expert-speak/nciipc-its-evolving-framework.

61 See, for example, the variety of security measures listed in the Indian government's "Guidelines for the Protection of National Critical Information Infrastructure" that have nothing to do with data residency and that can be implemented through licensing or contractual requirements with service providers. Also see Pranesh Prakash, "Why Data Localization Might Lead To Unchecked Surveillance," Centre for Internet and Society, October 15, 2018, https://cis-india.org/internet-governance/blog/bloomberg-quint-pranesh-prakash-october-15-2018-why-data-localisation-might-lead-to-unchecked-surveillance; and Matthias Bauer et al., "The Costs of Data Localisation: Friendly Fire on Economic Recovery," European Centre for International Political Economy, ECIPE Occasional Paper Series, 2014, 3, https://www.econstor.eu/handle/10419/174726.

62 Basu, Hickok, and Chawla, "The Localization Gambit," 39–40.

63 Interviews with respondents who wish to remain anonymous, on July 13, 2019.

64 While the bill creates categories of data that cannot be taken out of India under any circumstances (critical personal data), the bill leaves it to the central government to define this term. It is therefore possible that the central government may not define critical personal data at all._

65 For a summary of these variations, see Smriti Parsheera and Prateek Jha, "Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options?," Carnegie India, November 2020, https://carnegieendowment.org/files/ParsheeraJha_DataAccess.pdf.

66 See sections 33 and 34 of India's "Personal Data Protection Bill, 2019."

67 Roseanna W. Saaty, "The Analytic Hierarchy Process: What It Is and How It Is Used," *Mathematical Modelling* 9, no. 163 :(1987) 5–3, https://core.ac.uk/download/pdf/82000104.pdf.

68 Madhulika Srikumar, Sreenidhi Srinivasan, DeBrae Kennedy-Mayo, and Peter Swire, "India-US Data Sharing For Law Enforcement: Blueprint for Reforms," Observer Research Foundation, January 2019, 12, https://www.orfonline.org/wp-content/uploads/2019/01/MLAT-Book-_v8_web-1.pdf.

69 Srikumar, Srinivasan, Kennedy-Mayo, and Swire, "India-US Data Sharing For Law Enforcement," 8.

70 See for example, the U.S. law that prohibits sharing of content data with foreign governments without an order by a U.S. court. See "18 USC Ch. 121: Stored Wire and Electronic Communications and Transactional Records Access," U.S. House of Representatives, 18 U.S.C. §§ 2701 § (1986), https://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter121&edition=prelim.

71 See for example Srikrishna Committee of Experts, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, 88. The authors note, "In order to fulfil this mandate, law enforcement bodies often need to gain access to information that is held and controlled by data fiduciaries. As a result of this, it is important for the law to acknowledge the importance of quick and easy access to information to effectively secure national security and public safety."

72 See Kirtika Suneja and ET Bureau, "India Receives Highest Ever FDI in Apr-Aug FY21: Government," *Economic Times*, October 21, 2020, https://economictimes.indiatimes.com/news/economy/finance/india-receives-highest-ever-fdi-in-apr-aug-fy21-government/articleshow/78773388.cms?from=mdr; and ET Bureau, "FDI in Technology Sector Saw a 336% Rise in Apr-Sep 2020: Economic Survey," *Economic Times*, January 29, 2021, https://economictimes.indiatimes.com/tech/technology/fdi-in-technology-sector-saw-a-336-rise-in-apr-sep-2020-economic-survey/articleshow/80586966.cms.

73 Srikumar, Srinivasan, Kennedy-Mayo, and Swire, "India-US Data Sharing For Law Enforcement," 43.

74 See, Bhaskar Chakravorti, Ajay Bhalla, and Ravi Shankar Chaturvedi, "Which Countries Are Leading the Data Economy?," *Harvard Business Review*, January 24, 2019, https://hbr.org/2019/01/which-countries-are-leading-the-data-economy. This report finds the United States leading the world in "data production," followed by UK and China, while India is ranked twenty-fourth. Also see "China Holds More of the World's Data Than Any Other Country," *U.S. News and World Report*, February 14, 2019, https://www.usnews.com/news/best-countries/articles/2019-02-14/china-overtook-the-us-and-will-hold-the-largest-share-of-worlds-data-at-least-by-2025. It states that China, followed by the United States, holds most of the world's data. Lastly, see Srikrishna Committee of Experts *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, 89.

75 Srikumar, Srinivasan, Kennedy-Mayo, and Swire, "India-US Data Sharing For Law Enforcement," 43–44.

76 Bedavyasa Mohanty and Bedavyasa Mohanty, "The Encryption Debate in India," Carnegie Endowment for International Peace, May 30, 2019, https://carnegieendowment.org/2019/05/30/encryption-debate-in-india-pub-79213. For a general overview on issues related to encryption and national security, see Peter Swire, "From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud," *International Data Privacy Law* 2, no. 200 (April 12, 2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2038871&download=yes.

77 See Chapter 121 of the U.S. Stored Communications Act on stored wire and electronic communications and transactional records access. The act is a blocking statute and prevents U.S.-based service providers from disclosing content data to foreign governments, unless there is an agreement with the government under the U.S. CLOUD Act. This prohibition operates even if the foreign government seeks data regarding its own nationals in relation to a crime committed in the foreign government's jurisdiction.

78 The delay in access to data has been highlighted as the primary concern motivating discussions on law enforcement cooperation and reforms of existing protocols such as the MLAT framework. See, for example, Srikumar, Srinivasan, Kennedy-Mayo, and Swire, "India-US Data Sharing For Law Enforcement," 38–39.

79 Ibid, 19, 38.

80 See Articles 3 and 48 of the EU's GDPR law.

81 "Payment and Settlement Systems Act, 2007," Reserve Bank of India, Pub. L. No. 51 of 2007, 2007, https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/86706.pdf. See Section 4(1), which states that no payment system in India can operate without prior authorization from the Reserve Bank of India.

82 "Foreign Entities Getting Into Payment Systems in India," Vinod Kothari Consultants, August 27, 2018, http://vinodkothari.com/2018/08/foreign-entity-payment-system.

83 Jessica Shurson, "Data Protection and Law Enforcement Access to Digital Evidence: Resolving the Reciprocal Conflicts Between EU and US Law," *International Journal of Law and Information Technology*, 2020, 4–5, https://doi.org/10/ghnj29.

84 *CLOUD) Act*; and *18 U.S. Code § 2713*, Cornell Law School Legal Information Institute, https://www.law.cornell.edu/uscode/text/18/2713#:~:text=A%20provider%20of%20electronic%20communication,-subscriber%20within%20such%20provider's%20possession%2C.

85 See Clause 26(2) of India's "Personal Data Protection Bill, 2019." Significant data fiduciaries also include "social media intermediaries."

86 For example, see "The Technology 202: Activists Turn to Facebook Shareholders in Long-Shot Bid to Oust Zuckerberg," *Washington Post*, May 7, 2019, https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2019/05/07/the-technology-202-activists-turn-to-facebook-shareholders-in-long-shot-bid-to-oust-zuckerberg/5cd10b1b1ad2e506550b2f81; and Matthew Field, "Facebook Shareholders Revolt in Bid to Topple Mark Zuckerberg as Chairman," *Telegraph*, June 4, 2019, https://www.telegraph.co.uk/technology/2019/06/04/facebook-shareholders-revolt-bid-topple-mark-zuckerberg-chairman.

87 See, for example "Senator Hawley Introduces Bill to Address National Security Concerns Raised by Big Tech's Partnerships With Beijing," Office of U.S. Senator Josh Hawley, November 18, 2019, https://www.hawley.senate.gov/senator-hawley-introduces-bill-address-national-security-concerns-raised-big-techs-partnerships; and Sam Sacks, "Data Security and U.S.-China Tech Entanglement," *Lawfare*, April 2, 2020, https://www.lawfareblog.com/data-security-and-us-china-tech-entanglement.

88 Salman SH, "TikTok Users Shifting to Alternative Platforms yet to See Any Engagement: Report," *Mint*, July 12, 2020, https://www.livemint.com/companies/news/tiktok-users-shifting-to-alternative-platforms-yet-to-see-any-engagement-kalagato-report-11594557780995.html.

89 For example, see Ananya Bhattacharya, "TikTok Rip-Offs Fail to Gain Traction in India as Users Still Hope That Ban Will Be Lifted," Scroll.in, August 21, 2020, https://scroll.in/article/970927/tiktok-rip-offs-fail-to-gain-traction-in-india-as-users-still-hope-that-ban-will-be-lifted. The article states: ". . . But most of these Indian players struggled to deliver quality to new users who were flocking to them in hundreds. The influx in the first few days revealed weaknesses when the apps couldn't handle the load and kept crashing."

90 "Addressing the Threat Posed by TikTok, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain," (Trump) White House, Executive Order 13942 of August 6, 2020, https://www.federalregister.gov/d/2020-17699.

91 Neha Dasgupta, "U.S. Warns India Against Retaliatory Duties Over Scrapping of Trade Privileges," Reuters, May 7, 2019, https://www.reuters.com/article/us-usa-india-trade-idUSKCN1SD14M; and Mihir Sharma, "View: India Should Call a Truce in Its Trade Conflict with US," *Economic Times*, February 14, 2019, https://economictimes.indiatimes.com/news/economy/foreign-trade/view-india-should-call-a-truce-in-its-trade-conflict-with-us/articleshow/67987312.cms?from=mdr.

92 Kathuria, Kedia, Varma, and Bagchi, *Economic Implications of Cross-Border Data Flows*, 34.
93 See appendix 2 for more details.
94 The U.S. Cloud Act is one example of such a bilateral measure.
95 For details, see Parsheera and Jha, "Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options?"
96 See Section 4(1) of India's "Payment and Settlement Systems Act, 2007." Also see Vinod Kothari Consultants, "Foreign Entities Getting into Payment Systems in India."
97 See page ten for more information on this point.
98 Kathuria, Kedia, Varma, and Bagchi, *Economic Implications of Cross-Border Data Flows*.
99 Priyanka Sangani, "Data Centres May Prove to Be the Next Big Opportunity in India," *Economic Times*, October 23, 2019, https://economictimes.indiatimes.com/tech/internet/data-centres-may-prove-to-be-the-next-big-opportunity-in-india-/articleshow/71714171.cms; and "The Data Center Market in India Is Expected to Grow at a CAGR of Over 4% During the Period 2019-2025," CISION PR Newswire, April 17, 2020, https://www.prnewswire.com/news-releases/the-data-center-market-in-india-is-expected-to-grow-at-a-cagr-of-over-4-during-the-period-20192025-301042643.html.
100 Press Trust of India, "India's Data Consumption May Touch 25 GB/Month Per User By 2025: Ericsson," June 16, 2020, https://www.bloombergquint.com/business/india-s-data-consumption-may-touch-25-gb-month-per-user-by-2025-ericsson.
101 Celeste Clipp et al., "Digital Infrastructure and Economic Development: An Impact Assessment of Facebook's Data Center in Northern Sweden," Boston Consulting Group, June 2014, 4, 5, https://image-src.bcg.com/Digital-Infrastructure-Economic-Development-Jun-2014-Nordics_tcm22-29049.pdf.
102 Nam Pham, "Data Centers: Jobs and Opportunities in Communities Nationwide," SSRN, 2017, 12, https://www.ssrn.com/abstract=2998644. See table 9 on page 12.
103 For example, see "What Is the Economic Impact of Data Centers?," Dutch Data Center Association, https://www.dutchdatacenters.nl/en/data-centers/what-is-the-economic-impact-of-data-centers. The webpage states, "Data centers generate an enormous amount of employment, because they are part of a unique logistics chain consisting of all kinds of companies, from Internet exchanges, hosting- and cloud providers, to consulting firms and fiber optic providers. In total, around 5,000 FTEs are working directly in the data centers nationwide. … In total, Dutch data centers will create no less than 12,800 jobs in 2019, and this is estimated to grow to 16,800 in 2024."
104 Fletcher A. Mangum et al., "The Impact of Data Centers on the State and Local Economies of Virginia" Northern Virginia Technology Council, January 2020, 2, http://biz.loudoun.gov/wp-content/uploads/2020/02/Data_Center_Report_2020.pdf.
105 "Economic Impact of Data Centers on Central Washington," Washington Research Council, September 2013, 5, https://researchcouncil.files.wordpress.com/2013/08/datacenterssept2013.pdf.
106 Arpita Mukherjee, Soham Sinha, Angana Parashar Sarma, Nibha Bharti, and Drishti Vishwanath, "COVID-19, Data Localisation, and G20: Challenges, Opportunities and Strategies for India," Indian Council for Research on International Economic Relations *Working Paper* 398, October 2020, 17, http://icrier.org/pdf/Working_Paper_398.pdf.
107 Leviathan Security Group, "Quantifying the Cost of Forced Localization."
108 See the survey responses in Mukherjee et al., "COVID-19, Data Localisation and the G20," 25. Also see Sangani, "Data Centres May Prove to Be the Next Big Opportunity in India." The latter source states, "it is estimated that over 75% of this data now resides outside the country."

109 Srikrishna Committee of Experts, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, 92. The report states, "Creation of digital industry and digital infrastructure are essential for developments in AI and other emerging technologies, therefore highlighting the significance of a policy of requiring either data to be exclusively processed or stored in India. This benefit can be captured in a limited manner by ensuring that at least one copy of personal data is stored in India . . ."

110 For example, see "How to Flourish in an Uncertain Future: Open Banking and PSD2," Deloitte, 2017, 11, https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-open-banking-and-psd2.pdf. The report states, "The opening up of data may also drive competition in other products. This is because it would mitigate one of the prime advantages enjoyed by incumbent banks: access to historical transaction data, which commonly allows incumbents to provide better offers on credit products, particularly for SMEs. Opening up this data to third parties would clearly level the playing field."

111 Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" Information Technology and Innovation Foundation, May 2017, http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.221739544.1252223219.1606218014-500694206.1606218014.

112 Marg and Park, "Data Localisation: India's Double-Edged Sword?," 28.

113 David Autor et al., "The Fall of the Labor Share and the Rise of Superstar Firms*," *Quarterly Journal of Economics* 135, no. 2 (May 1, 2020): 645–709, https://doi.org/10/ggw39f. In particular, see page 703.

114 For example, see Mukherjee et al., "COVID-19, Data Localisation, and the G20," 26.

115 See appendix 3.

116 For more information on the funders of Carnegie India's Technology and Society Program, see the following website: https://carnegieindia.org/specialprojects/technologyandsociety.

United C-5 & 6 | Edenpark | Shaheed Jeet Singh Marg | New Delhi, India 110016 | P: +011 4008687

CarnegieIndia.org