



30 September 2018

Joint Secretary
Ministry of Electronics and Information Technology ("MeitY")
Room No. 4016, Electronics Niketan,
6 CGO Complex, CGO Complex,
Lodhi Road,
New Delhi – 110 003.

**Sub.: Submission of response to the draft Personal Data Protection Bill, 2018
("Draft Law")**

Dear Madam/ Sir,

We are grateful to the MeitY for creating an opportunity to engage with the Indian authorities on the Draft Law. With India at the forefront of the global technology ecosystem, we find that this discussion around the Draft Law timely and imperative.

The Asia Internet Coalition (AIC) is an industry association made up of leading internet and technology companies. The AIC seeks to promote the understanding and resolution of Internet policy issues in the Asia region. Our members include AirBnB, Amazon, Apple, Expedia, Facebook, Google, LinkedIn, LINE, Rakuten, Twitter and Yahoo (Oath).

As responsible stakeholders in this process, we appreciate the ability to participate in this public consultation process. In this submission, we identify the overarching concerns with data localization norms, as proposed in the Draft Law, and recommend the way forward for a uniform regime that incentivizes an environment with consumer choice and access as the key drivers.

We would also be happy to offer our inputs and insights directly through meetings and discussions with the relevant authorities. Do reach out to us at jamie@aicasia.org.

Regards,

A handwritten signature in blue ink, appearing to read "Jeff Paine", written in a cursive style.

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

The Impact of the 2018 Draft Personal Data Protection Bill on India's Economy, Business and the Public

INTRODUCTION

Globally, technology innovation is being driven in a location agnostic manner. All leading technology platforms – social media, search, information dissemination, travel, e-commerce, payments, professional networking, etc. – have historically been created and offered across the globe, and continue to have the technical ability to be offered without restriction or discrimination on the regions served. In such an ecosystem, measures such as data localization are likely to be considered protectionist and barriers to free trade. In the following sections, we illustrate certain glaring challenges of data localization norms.

WHAT THE DRAFT LAW PROPOSES

The Draft Law requires that every data fiduciary maintain at least one serving copy of personal data on a server/ data centre in India, although the central government may grant exemptions based on necessity and strategic interests of the State. Such exemption shall not apply to sensitive personal data. Critical personal data (which the Data Protection Authority (“DPA”) may notify) shall only be processed on a server/ data centre in India. This is a stark departure from the provisional views of the Justice Srikrishna Committee, as stated in the November 2017 White Paper of the Committee of Experts on a Data Protection Framework for India, which acknowledged and accepted that a blanket localization requirement may not be in the best interest of the goals of the Indian economy. Additionally, personal data may be transferred outside of India, subject to approved standard contractual clauses or inter-group schemes, permitted countries, specifically permitted transfers, and consent.

CHALLENGE 1: NEGATIVE ECONOMIC IMPACTS

Restrictions on cross border data flows pose a threat, from both a macro and micro economic perspective, to individual businesses and economies at large. The free flow of data across borders makes businesses produce goods and provide access to services efficiently.

The negative economic impact of restricting cross border data flows is well documented under various studies – for instance, a 2014 ECIPE study¹ determined the impact of existing data privacy and security legislation on GDP: Brazil (-0.2%), China (-1.1%), EU (-0.4%), India (-0.1%), Indonesia (-0.5%), Korea (-0.4%) and Vietnam (-1.7%). If these countries also introduce economy-wide data localization requirements, GDP losses would be even higher: Brazil (-0.8%), the EU (-1.1%), India (-0.8%), Indonesia (-0.7%), Korea (-1.1%). The impact on overall domestic investments is also considerable: Brazil (-4.2%), China (-1.8%), the EU (-3.9%), India (-1.4%), Indonesia (-2.3%), Korea (-0.5%)

¹ <http://ecipe.org/publications/data/loc/>; http://www.ecipe.org/app/uploads/2014/12/OCC32014_1.pdf

and Vietnam (-3.1). In the context of welfare losses, for India, the estimated loss per worker is equivalent to 11% of her average monthly salary. The study also stated that a data localization measure at the time in India would have reduced projected growth by approximately 20%, while also causing a (-)1.9% drop in domestic and foreign investments that drive long term growth. The study concludes that enforcement of cross-sectoral localization laws in India would impact the economy negatively by “decreasing productivity, hampering exports and discouraging investment”.²

A McKinsey report published in 2016³ posited that global flows of all kinds increase productivity as they positively impact and support growth. It further stated that this effect is greatly amplified by cross border data flows as they increase participation and efficiency within markets. The study determined a 10.1% rise in global GDP over a decade, directly as a result of cross border data flows. **“This value amounted to some \$7.8 trillion in 2014 alone, and data flows account for \$2.8 trillion of this impact.”** Growth is equally impacted by data flowing in and out of economies – these flows invite and integrate ideas, research, technologies, talent and best practices from the world over. *Au contraire*, imposition of localization norms establish heavy obligations and costs for compliance.

Historically, India’s IT industry has thrived owing to its customers (like the United States) embracing an open and permissible ecosystem of cross border data transfers. Resultantly, India is hailed as one of the biggest sourcing destinations of the world, accounting for nearly 67% of the approximately USD 130 billion market, with a workforce of roughly 10 million.⁴ It is also important to remember that the negative impacts of data localisation do not end with the internet industry – another McKinsey study estimates that the impact of unhindered data flows in the Internet of Things (IoT) across healthcare, urban infrastructure, manufacturing, security, agriculture, electricity, retail etc. shall be approximately USD 2.7 to USD 6.2 trillion per year.⁵

From a broader perspective, we note from extensive studies that cost of regulation percolates down to the end consumer – i.e. the common person. Economic growth and entrepreneurship suffer at the cost of regulation.⁶ According to a study⁷, US federal regulations reduced economic growth by about 2% each year between 1949 and 2005. The study determined that if the level of federal regulation was frozen in 1949, the then-current GDP, in 2013, would have been USD 38.8 trillion higher. Unnecessary top-down government intervention and regulation should give way to self-governance which is less expensive and invasive; the cost of regulation trickles down to the consumer, or reduces the regulated entity’s profits, until doing business is impossible. Neither should constitute a regulatory goal for the Draft Law.

² http://ecipe.org/publications/data/doc/; http://www.ecipe.org/app/uploads/2014/12/OCC32014_1.pdf

³ McKinsey Global Institute, Digital Globalization: The New Era of Global Flows, March 2016, <https://www.mckinsey.com/~media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx>

⁴ <https://www.ibef.org/archives/detail/b3ZlcnZpZXcmMzcwMDQmODk=>

⁵ http://www.mckinsey.com/insights/business_technology/disruptive_technologies

⁶ <https://www.usnews.com/opinion/blogs/economic-intelligence/2013/08/27/regulations-cost-the-us-economy-trillions-of-dollars>

⁷ <http://www4.ncsu.edu/~jjseater/regulationandgrowth.pdf>

CHALLENGE 2: LOCAL STORAGE ≠ SECURITY, PRIVACY, LAWFUL ACCESS

The proposition that local storage of data strengthens privacy and security imperatives is a myth. It has been argued that the notion that data is required to be stored locally for ensuring privacy and security is fallacious.⁸ There is no empirical evidence that vouches for increased security benefits as a result of restricting cross border flows or forced localization laws in any manner.⁹

From a business perspective, storing data across jurisdictions offers the immense benefit of ensuring business continuity and reliability, especially during infrastructural outages, natural disasters or political upheaval. Furthermore, localization laws are criticized world over for being used as tools to curb free speech or to target dissidents, and force service providers to comply with law enforcement directives around surveillance, monitoring, interception etc.¹⁰ Security may, technically, be ensured by using measures such as end-to-end encryption, international security standards such as the IS/ISO/IEC codes, the use of distributed servers in a location agnostic manner etc.

As far as the question of lawful access is concerned, we recommend strengthening domestic skill sets and international processes – both bilateral and multilateral – in order to facilitate the flow of information for law enforcement purposes. Merely locating data domestically does not automatically enable or increase access to information for legitimate law enforcement purposes – that would depend upon legal principles and judicial precedent around privacy rights and due process. The regulatory hope that forced localization would permit unfettered law enforcement access to data is unreasonable, flawed and not achievable. It appears, from public discourse, that the major driving force for localization in India is lawful access. As outlined here, lawful access is in no way guaranteed by forced localization; although the negative economic and innovation impacts are.

CHALLENGE 3: INNOVATION OBSTRUCTION

Barriers to cross border data flows, as caused by localization laws, are globally understood to have negative impacts on innovation and availability of/ access to the best of a set of competing services to end users.

By way of an example, cloud computing has proved to be an affordable, and therefore cost-efficient, option for businesses (especially startups, small and medium businesses). This is largely on account of the reliance placed by cloud computing on colossal economies of scale and globally distributed data centres. A 2016 report published by the Internet and Mobile Association of India (“IAMAI”)¹¹ specifically illustrates the impact of high cost barriers such as localization norms as being discouraging of innovation, particularly in the small and medium enterprises segment.

⁸ Daniel Castro, The False Promise of Data Nationalism, INFO. TECH. & INNOVATION FOUND. 1 (Dec. 2013), <http://www2.itif.org/2013-false-promise-data-nationalism.pdf>

⁹ http://report.analysismason.com/DDI_Emerging_APAC/DDI%20in%20emerging%20APAC%20-%20Final%20report%20-%202016%2008%2006%20-%20FINAL.pdf

¹⁰ <https://www.accessnow.org/the-impact-of-forced-data-localisation-on-fundamental-rights/>

¹¹ http://www.iamai.in/sites/default/files/position_papers/make-in-india.pdf

Forced localization, by way of direct implication, would result in businesses losing access to the most economically efficient option for locating and/ or processing their data in a geographically agnostic manner. As operational and maintenance costs drive up, and where resources are limited in the first place), innovation, research and development are the most likely to suffer. The 2015 Leviathan Group study¹² indicates that mandatory localization requirements increase costs to local businesses by 30% to 60%, as opposed to companies that are able to conduct their business with unobstructed cross border data flows.

Private sector studies are not alone – in 2018, the Telecom Regulatory Authority of India (“TRAI”), in its consultation paper on *Privacy, Security and Ownership of the Data in the Telecom Sector*¹³ stated that over-regulation, such as data localization, can adversely affect innovation, creativity and competition in the sector, and would serve as a barrier to setting up of the new internet or mobile telephony-based businesses and services along with adversely affecting the growth of the technology based startup sector in India.

The re-channelization of funds to locate data locally eats into innovation/ R&D budgets. Services developed and offered based on data stored in foreign jurisdictions becomes challenging to offer in India in a seamless and frictionless manner. The most jarring impact of the *forced localisation* – innovation obstruction paradigm is that the Indian consumer is robbed of the opportunity to access leading and innovative offerings.

CHALLENGE 4: INDIA’S INTERNATIONAL TRADE LAW OBLIGATIONS

We also take this opportunity to point out that data localization results in the creation of trade barriers, which may be seen as a failure of India’s fulfilment of its obligations under regional and international trade laws.¹⁴ The General Agreement on Trade in Services regime enshrines criteria around objectivity and reasonableness in domestic-protectionist measures, and it is unlikely that the provisions of the Draft Law would pass the tests therein.

It may also be useful to also bear in mind that various developed economies are, world over, engaging with one another on the principle of cooperation, and not forced domestic storage of data. This includes participation in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), Regional Comprehensive Economic Partnership (RCEP) as well as APEC Cross Border Privacy Rules (CBPR). These multilateral processes find their basis in the understanding that cross-border data flows are quintessential to global economic growth, and that cooperative measure enable such cross jurisdictional data flows while protecting privacy

¹²

<https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf>

¹³ TRAI Consultation paper on Privacy, Security and Ownership of the Data in the Telecom Sector (2018); available at https://trai.gov.in/sites/default/files/IAMAI_07112017.pdf

¹⁴ Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments, Daniel Crosby; available at: <http://e15initiative.org/wp-content/uploads/2015/09/E15-Policy-Brief-Crosby-Final.pdf>

and respecting international trade law obligations. We recommend that India considers partaking in these processes, as opposed to enforcing protectionist measures like a forced localization law.

CHALLENGE 5: INFRASTRUCTURAL IMPEDIMENTS

India does not have a flourishing data centre ecosystem. It is worthwhile to bear in mind that even the available data centres primarily operate on a co-location model¹⁵ – i.e. where the consumer of the data centre bears the infrastructural and cost requirements of actually setting up servers and storage, and the co-location entity provides ancillary services like bandwidth, cooling, physical security and space. Therefore, at present, India lacks the appropriate infrastructure to sustain an ecosystem based on local data storage.

In other words, a burgeoning cloud computing industry with localized storage would need to precede any localization law. To set up and maintain such a system, the costs involved are mammoth. A study on the risk index for establishing data centres¹⁶ estimates the cost of setting up server farms in Brazil at USD 60.9 million, contrasting with USD 51.2 million in Chile and USD 43 million in the US. According to this study, the operational costs and other expenses per month can be as high as USD 950,000 in Brazil, USD 710,000 in Chile and USD 510,000. India, incidentally, was identified by this study as one of the riskiest countries for setting up and operating data centres. While the study recognizes the opportunity in India, it considers significant barriers to the ease of doing business, especially power security concerns, as the primary reason for India being identified as the highest risk economy in the APAC region.

It may be instructive to also learn from the findings of a study by the Leviathan Group study in 2015¹⁷ –

- Averaged across the types of servers, a customer located in Brazil would pay 54.65% less by using cloud servers outside Brazil, rather than requiring only Brazil-located cloud computing resources.
- In the UK and Ireland, the locally available data centres are consistently at least 56.5% more expensive than their counterparts elsewhere in the world. Businesses that move their servers outside this region could thus save more than 36% on their server costs.
- At 4GB and above, the cheapest servers in the Schengen Area are consistently 10.5% more expensive than the lowest-cost alternatives worldwide.

¹⁵ <https://www.datacentermap.com/india/>; also see <https://www.wp-tweaks.com/list-indian-web-hosts-data-centers-india/>

¹⁶ CUSHMAN & WAKEFIELD, DATA CENTRE RISK INDEX (2013), <http://www.cushmanwakefield.com/%20~/media/global-reports/data-centre-risk-index-2013.pdf>

¹⁷

<https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf>

By way of an example, an Indian technology services company stated¹⁸ (in its IPO offer document) that the estimated cost for purchasing equipment to establish a Tier-III data centre in a special economic zone would be INR 752 million (approximately USD 103.8 million). The actual cost would, of course, be a multiple of this amount, to account for costs related to land and statutory expenses (the document estimates the total expense at over INR 3.5 billion, i.e. approximately USD 0.5 billion), and once established, ongoing operational and maintenance charges.

Power continues to be a challenge even today in a 2018-India. In 2014, the US reportedly witnessed a power consumption of more than 70 billion kilowatt hours of electricity only to power local data centres, which was 2% of the national energy consumption; by 2020, 20% of the world's energy is expected to be consumed by data centres!¹⁹ By contrast, in 2015, India's per capita power consumption was only 1010 kilowatt hours,²⁰ almost half of the global average.²¹ According to publicly available sources, 32 million households in India do not have electricity.²² In a power deficit country like India, where national demand for electricity is underwhelmingly underserved by a sparse supply, diverting such limited supply to establish and maintain data centres (especially where alternatives are available overseas) at the cost of essential access to the urban and remote populace, appears to be almost cruel.

Power is far from being the only infrastructural challenge for the data centre industry. The provision of server services is equally reliant upon connectivity. With nearly 1.2 billion subscribers,²³ India is the world's second largest telecommunications market.²⁴ The telecommunications sector in India is heavily regulated, spectrum is limited, right of way permissions are challenging, and both the industry and regulator are still trying to address concerns around ease of doing business. With a lengthy and compliance-heavy regulatory and licensing process, as well as limitation in the availability of resources, we believe India is yet to achieve the optimal position to be ready to host a local storage ecosystem.

CHALLENGE 6: REGULATORY CONCERNS

Overall, we note that the Data Protection Authority ("DPA"), which is the proposed regulatory body under the Draft Law, bears extensive responsibilities and wide discretionary powers. This includes cases where the DPA may determine whether or not certain data is required to be mirrored in India, the power to review and permit contracts, schemes and countries for cross border data transfers, and (inter alia) categorization of specific kinds of personal data as well as the levels of protection/ local storage requirements thereto. The DPA, we note, shall itself be a newly created regulator under the Draft Law, and the exercise of such far reaching discretionary

¹⁸ p.103, https://www.sebi.gov.in/filings/public-issues/mar-2016/infibeam-incorporation-limited_31886.html

¹⁹ http://timesofindia.indiatimes.com/articleshow/65818770.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

²⁰ World Bank, CEA, EIA, CRISIL Research, read in <https://www.goldmansachs.com/worldwide/india/ipo/renew-power-limited/drhp.pdf>

²¹ p.125, <https://www.goldmansachs.com/worldwide/india/ipo/renew-power-limited/drhp.pdf>

²² Saubhagya Dashboard (2018); available at <http://saubhagya.gov.in>

²³ Saubhagya Dashboard (2018); available at <http://saubhagya.gov.in>

²⁴ Saubhagya Dashboard (2018); available at <http://saubhagya.gov.in>

powers by a new regulator, if not preceded by appropriate guidance/ training modules, has the potential of creating regulatory uncertainty and standardization challenges.

Separately, it may also be useful to bear in mind that the constitution document²⁵ that established the Justice Srikrishna Committee outlined its functions as studying issues around data protection in India and suggesting principles behind data protection and related legislation in India. We've established in the earlier sections that there is no evidence of a nexus between localization laws and data protection, and therefore, we posit, that the committee proposed forced localization in excess of its mandate, and that localization, as a normative approach, should not be part of the country's privacy and data protection legislation, which is what the Draft Law is.

CONCLUDING REMARKS

The business decision on where an enterprise chooses to locate data is based on a variety of parameters, including power infrastructure, connectivity, legal frameworks, ease of doing business, global integration, law and order and political stability. Making data localization a forced reality does not automatically create a business case for optimal avenues financially, technically and operationally. MeitY's working group on cloud computing (under the Chairpersonship of Kris Gopalakrishnan)²⁶ is also reported to be deliberating upon the establishment of data localization norms. The group, it appears, is tasked with establishing an incentives-based framework for enabling the cloud computing industry within India.

All the challenges outlined here in our submission apply to all instances of locating data domestically, and impact mirroring and exclusive local storage requirements equally. Therefore, we recommend that the Draft Law reassess data localization within the Indian context, and approach it from an incentivization perspective, as opposed to a regulation-heavy framework. An incentive-based policy, we believe, would be a step in the right direction. Government policies that incentivize and create empowering frameworks to build and maintain an ecosystem that makes it efficient and viable to locate data in India, without forced restrictions or requirements to statutorily locate such data within the Indian jurisdiction, would serve both the policy and business imperatives in the most optimal manner. We would applaud and participate in any policy efforts that are aimed towards encouraging a sustainable and organic path to creating a data centre economy within India.

²⁵ http://meity.gov.in/writereaddata/files/meity_om_constitution_of_expert_committee_31072017.pdf

²⁶ p.23, DSCI Annual Report 2017-18; available at https://www.dsci.in/sites/default/files/documents/resource_centre/Annual-Report-2017-18.pdf