NUS National University of Singapore | ISAS Institute of South Asian Studies

ISAS Insights
No. 579 – 4 September 2019

The Battle over India's Data Policy Framework: What Gives?

Karthik Nachiappan

Summary

Debates related to data localization are front and centre in India. India's draft data legislation – the Personal Data Protection Bill that centred on localization with provisions extended to the protection of personal data appears to be on the cusp of being altered. This paper analyses how considerations at three different levels – global, national and subnational affect discussions on the newly proposed data bill that must reconcile factors related to security, innovation and accessibility. How Indian officials resolve this knot will give us an idea of the values underpinning India's approach toward technology policies.

Introduction

A fierce battle is brewing over India's data policy – the Personal Data Protection Bill. It is shaping up to be a clash where priorities related to innovation, jobs and development clash with security, access and control. The politics around India's data policy has clear global, national and sub-national dimensions. New Delhi must adroitly manage pulls from these directions to enact a data protection law that gives citizens adequate protections vis-a-vis data use and transfer and businesses, foreign and domestic, the space to deploy data to service customers and create new jobs and services. New rules will also have to straddle security concerns since government agencies would prefer reliable access to data. These competing pressures will affect India's data protection law. How prevailing trade-offs around data flows get resolved will shed light on what values drive India's approach toward technology issues.

Global Data Governance

There is limited global coordination on establishing robust standards on data flows. The absence of norms around which domestic data rules can be crafted has generated uncertainty. There appears to be little progress on the normative front. At the 2019 G20 Summit, host Japan introduced a 'Data Free Flow with Trust' (DFFT) system to facilitate free flow of data under acceptable global rules. Prime Minister Abe's DFFT concept revolved around two pillars – first, personal and 'sensitive' data is to be placed "under careful protection" and second, for "medical, industrial, traffic" to flow across borders for economic purposes. Through this approach, Abe sought to create a baseline for data rules that protects privacy and enables data sharing.[1] But the Japanese initiative was hamstrung by differences between industrialized countries, with Japan and the US supporting free flow, and emerging

[1]Government of Japan. Speech by Shinzo Abe, Japanese Prime Minister. May 30, 2019. https://japan.kantei.go.jp/98_abe/statement/201905/_00002.html

countries like China, India, Brazil and Russia, resisting.[2] Emerging countries endorsed data localization while the OECD states preferred data flows with some constraints given relevant privacy concerns.

Divisions exist. The United States will reject international rules that place constraints on its technology companies. China, in contrast, has become the G20's most pronounced digital protectionist, placing curbs on cross border data flows alongside stringent rules on companies looking to enter China. India has been hawkish on data flows, proposing several restrictions on data use and transfer. Other G20 countries like Indonesia, Turkey, South Korea and Saudi Arabia also have some data localization laws. This profound gulf could constrain future multilateral discussions on data governance. The DFFT's innate weakness was that it did not comport with domestic political currents across the world that have become allergic towards unconstrained data flows. That said, the establishment of a globally relevant data standard brings certainty – allowing countries to provide somewhat symmetric levels of data protection and privacy to their citizens while empowering businesses to streamline business operations.

Given fault lines between major powers, international organizations are under pressure to develop robust data standards. Calls have now increased for the WTO to place digital flows under its Integrated Trade Intelligence Portal which compiles information on how countries manage their trade policy. Indeed, Prime Minister Abe identified the WTO as the site where global data standards should be established, prodding WTO officials to expand the trade remit. Though WTO rules bar measures like data protections which constrains trade, exceptions exist within the General Agreement on Trade in Services (GATS) for various domestic policies that do not comport with GATS provisions. Some technology companies are pushing the US to use the WTO to challenge China's controversial data laws where data flows are used for censorship and surveillance.[3] In fact, China has used exceptions in the GATS agreement to defend its data management approach claiming those measures are "necessary to protect public morals and to maintain public order."[4] That said, the WTO could include data under its focus on e-commerce rules which are now being updated in Geneva.[5] Surprisingly, the World Bank has advocated for developing countries to establish data processing centres that could boost the creation of IT-based industries. Going ahead, the Bank will advise on how data fits into national business indicators, highlighting policy and regulatory issues around the digital economy.[6]

Multilaterally, two issues with respect to data governance must be addressed - which regime should draft global data rules and what principles should frame new rules, those that support data flows, with some constraints, or not. How this process plays out will impact India's data policy given the growing importance of the digital economy to global commerce.

---

[2]Ibid.

[3]Technode. "Dust yet to settle on China's cybersecurity law." June 10, 2019. https://technode.com/2019/06/10/dust-has-yet-to-settle-two-years-after-chinas-landmark-cybersecurity-law/

[4] Government of the United States. Office of the US Trade Representative. 2018 USTR report to Congress on China's WTO compliance. https://ustr.gov/sites/default/files/2018-USTR-Report-to-Congress-on-China%27s-WTO-Compliance.pdf

[5] Hurst, Daniel. "Japan calls for Global Consensus on Data Governance," The Diplomat. February 2, 2019.

[6] Cory, Nigel. "Cross border flows: Where are the barriers, and what do they cost?," Information Technology and Innovation Foundation Report. May 2017.

The absence of a global Internet protocol has generated territorial claims on data protection. Countries are trying to exert some control over data flows. The policy approaches of three key jurisdictions – the US, the EU and China matter since their standards shape the laws of countries they trade with. Market power drives regulatory harmonization and compliance. Currently, the US does not have a federal law on data protection. Instead, Washington relies on a 'sectoral' data protection approach through a combination of legislations, regulations and self-regulation.[7] The approach relies on businesses to front data protection. In addition, states like California, Ohio and Tennessee are crafting their own privacy laws given public demand. Protections, particularly that of citizen privacy, vis-a-vis data use, consumption and transfer, underpin the EU's privacy law – the General Data Protection Regulation (GDPR).[8] China's cybersecurity law requires data providers or 'network operators' to hold data collected within China inside its territory.[9]

India's data bill prioritizing innovation, security and protection contains provisions that exist in the approaches adopted by the US, EU and China. India's bill incorporated certain aspects of the GDPR, particularly provisions strengthening protections for data use and stipulating what companies can do with personal data. And like China, India's bill contains robust data localization requirements. But a tussle between data sharing and retention threatens this balance. Growing demands from the US to reverse the course on data localization, given US economic interests, particularly American technology companies, has pushed New Delhi to relax its stance on localization.[10] So far, American companies like Facebook, Amazon and Google have made India a key priority for their growth, establishing major operations across the country. Moreover, their success has largely been driven by harvesting, analysing and sharing the data of Indian citizens for commercial purposes. India's initial push toward localization sought to correct this trend with the data protection bill and related measures, pitting foreign tech behemoths versus domestic regulators and firms. New Delhi's sudden pushback suggests that India's trade relations with the United States will influence domestic data policy preferences that instinctively bend toward localization.

Push for Data Localization

In India, the demand for data rules anchored on localization is institutionally driven. Localization enables data access. The BN Srikrishna committee that issued a report on data protection, on which India's draft data law is based, recommended localization to safeguard data access.[11] The bill fleshed out a workable data regime by distinguishing between kinds of data ('personal' or 'sensitive personal' data) and spelling out the responsibilities of those that

[7] Boyne, S. "Data Protection in the United States," *The American Journal of Comparative Law*, Volume 66, Issue suppl_1, July 2018, Pages 299–343.
[8] Albrecht, Jan Philipp. "How the GDPR will change the world." *Eur. Data Prot. L. Rev.* 2 (2016): 287.
[9] Lindsay, J. R. (2015). "The impact of China on cybersecurity: Fiction and friction," *International Security*, *39*(3), 7-47.
[10]Indian government likely to cave on data localisation after pressure from the US. *New Tech for Old India.* https://www.zdnet.com/article/indian-govt-likely-to-cave-in-on-data-localisation-stance-after-pressure-from-us/
[11]Government of India. "A Free and fair digital economy: Protecting privacy, Empowering India," BN Srikrishna Committee Report. https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

use these data categories.[12]However, the trend towards localization in India, however, predate these new policies. Data protection provisions go back to the 2000 Information Technology (IT) Act and the 2011 Information Technology Rules that defined sensitive data and clarified norms for data collection.[13] With limited broadband penetration and wireless usage, despite a services-based economy, there was limited impetus to facilitate open data flows. Instead, the reverse desire to hold data continued through successive government measures.

In 2012, India enacted a National Data Sharing and Accessibility Policy (NDSAP) that mandated all government data be stored in local data centres.[14] In 2014, India's National Security Council instituted data localization, requiring all email providers to establish local servers for their India operations.[15] And in 2015, India's Ministry of Electronics and Information Technology (MEItY) obliged cloud providers seeking government contracts to store all relevant data in India.[16] The meteoric rise of digital financial flows and the intermittent use of foreign platforms to conduct transactions has bolstered localization. In April 2018, the Reserve Bank of India (RBI) mandated withholding payment data even if payments are processed outside of India to the annoyance of companies like Visa, Mastercard, Amazon and PayPal.[17] Data access, for Indian officials, serves as a bulwark against cybersecurity threats. Moreover, localization provides government officials control over data when required instead of requesting or waiting for it from external sources. This preoccupation will constrain India's data policy given cybersecurity risks to the state and citizens.

A need for data storage also reinforces localization. The storage angle is being pushed by Indian states who view data policy through the lens of jobs and development. Uttar Pradesh (UP) could become the first Indian state to compel technology companies like Amazon, Facebook and Flipkart to store data of their residents within the state.[18] UP plans to store data in newly constructed data centres that they hope will generate new jobs. Whether enough jobs will be created from data storage centres is an open question; moreover, doubts exist on whether Indian states can run such data centres. Notwithstanding these qualms, other states like Andhra Pradesh and Telengana are exploring new data centres to house their data.[19] A key factor driving this push within Indian states is the rapid penetration of 4G technology that has caused a dramatic rise in wireless data usage given dropping costs. These states believe storage and localization could force high-tech companies to shift activity

[12]Personal data includes information that can identify individuals while sensitive personal data covers specific information of individuals including health, gender, sexuality, religion, caste, etc. See the Srikrishna report.
[13]Bailey, R and Smriti Parsheera. "Data localisation in India: Questioning the means and ends," NIFPF Report. National Institute of Public Finance and Policy.
[14]Government of India. National Data Sharing and Accessibility Policy. http://dst.gov.in/national-data-sharing-and-accessibility-policy-0
[15]Bailey, R and Smriti Parsheera. "Data localisation in India: Questioning the means and ends," NIFPF Report. National Institute of Public Finance and Policy.
[16]Ibid.
[17] Reserve Bank of India. Circular on storage of payment system data. https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244
[18] The New Indian Express. "Noida may get centre to store app user data," August 22, 2019. http://www.newindianexpress.com/cities/delhi/2019/aug/22/noida-may-get-centre-to-store-app-user-data-2022606.html
[19]Ibid.

to within their borders. This strategy obliges these companies to generate value to local economies if they are keen on gathering and using the data of Indian citizens.

The economic benefits from local data processing and storage appear to be large. Having fully functional data processing centres could power India's growth over the long run. India's digital economy generates US$200 billion (S$278 billion) per year largely from digital services covering activities like business process management, digital communications, e-commerce, digital payments and direct subsidy transfers.[20] Estimates suggest India can create over US$1 trillion (S$1.3 trillion) of economic value from the broader digital economy by 2025 from these services and other sectors should they digitize as expected.[21] Currently, sectors like health, agriculture, logistics, education and energy do not have technology drive their operations but potential exists to change how they operate. This potential digital revolution could create a vast market space encompassing digital services, platforms, applications, content and solutions. Making data available, as a result, could catalyse digital entrepreneurship.

The latter desire is reflected in India's proposed e-commerce policy that imposes restrictions on cross border data flow. The e-commerce policy extends to cover a whole range of data provisions that affect digital commerce - source codes, data monetization, payments, intellectual property rights, privacy, data anonymization and search engine regulation.[22] The vast expanse of the e-commerce policy suggests that the Modi government views e-commerce openly, not purely in terms of digital transactions but as an infrastructural issue that could transform India's economy via digitization. New data facilities could spawn firms in areas like artificial intelligence, 3-D printing, IoT systems, robotics, analytics and data intelligence, generating new industries and jobs across the country.[23] Should these firms rise, they will support sovereign data rules that protect their interests. These domestic political factors will affect India's data policy that could seesaw between more and less localization.

India's data policy will confront various pressures at global, national and state levels where security, economic and political considerations intersect. Undeniably, the resultant design of India's data policy will impact India's economy (pace of innovation and productivity, digital ecosystems and jobs) and foreign policy (India's relations with the US, EU, China, Japan and countries across Southeast Asia). It will be interesting to see what gives.

. . . . .

Dr. Karthik Nachiappan is Research Fellow at the Institute of South Asian Studies (ISAS), an autonomous research institute at the National University of Singapore. He can be contacted at isaskn@nus.edu.sg. The author bears full responsibility for the facts cited and opinions expressed in this paper.

[20]The Hindu Businessline. "Digital Economy a $1 trillion opportunity for India," February 20, 2019.
[21]Radu, S. "India is the world's second fastest digitizing economy," US News and World Report. April 19, 2019.
[22]The Hindu Businessline. "Government releases draft e-commerce policy," February 23, 2019.
[23]Rizvi, Karim. "Why India's new e-commerce policy needs a relook," The Entrepreneur India, April 4, 2019. https://www.entrepreneur.com/article/331751