DIPLOMAT (Magazine)
February, 2020

The Retreat of the Data Localization Brigade: India, Indonesia, and Vietnam

The protagonists of the data localization saga in all countries have been similar and the tussle has proceeded along similar lines.

By Arindrajit Basu

2019 saw a major global tussle come into view over the regulation of cross-border data transfers, with a number of emerging economies taking measures to exercise greater sovereign control over their data. Contention on this issue is a product of a desire among emerging economies to push back against exploitative economic systems adopted by U.S.-based technology companies and mend a cumbersome process for law enforcement agencies seeking to access data stored in the United States. A key strategy adopted by these countries has been data localization mandates – a range of measures providing for mandatory storage or processing of data within the territory of a given country.

A major stakeholder in the political ecosystem surrounding data localization debates has been the Western lobby representing the interests of technology companies based in the United States. Through concerted efforts made in conjunction with both industry-led lobbying groups and state-backed diplomatic efforts they have managed to push emerging economies into diluting the scope of their data localization mandates and easing the restrictions on the free flow of data.

Last March, I co-authored a study that tracked all data localization mandates across the globe and identified China, India, Indonesia, and Vietnam as the key Asian countries that had existing or proposed laws mandating data localization in some form. With the exception of China (which has not altered its rigid data localization laws) the other three have all reneged on their respective localization gambits, to some extent.

This piece traces the narrowing localization provisions in three critical emerging economies – India, Vietnam and Indonesia – and studies the actors and geopolitical tussle that shaped these provisions.

Narrowing Data Localization Provisions

India

India's data localization gambit started in April 2018 when the Reserve Bank of India issued a directive to all companies to store data related to payments systems in India. WhatsApp Pay, Google Pay, Mastercard, and other foreign companies that deal with payment data are attempting to comply with this directive on priority. Since then there have been eight sectoral notifications mandating data localization in some form, from sectoral regulators governing insurance, healthcare, and e-commerce data.

The big global talking point was the introduction of a mirroring provision that mandated a live serving copy of all personal data be stored in India in a draft of the Personal Data Protection Bill that was made public in August 2018 along with a restriction of any cross-border data transfers for all data notified as "critical personal data."

When a revised version of the bill was finally introduced in parliament in December 2019, the mirroring provision was gone.

In its current form, the bill now only requires the storage of "sensitive personal data" within India, a subset of what was within the previous mandate. Sensitive personal data can also be transferred abroad for the purpose of processing upon the fulfillment of certain conditions – including obtaining explicit consent from the data user (called "data principal") and being in pursuance of a contract or an intra-group scheme that safeguards user rights, while also ensuring liability on the data processor (fiduciary) if harm does accrue.

Alternatively, "sensitive personal data" may be transferred abroad if the data is to be accorded an adequate level of protection in that jurisdiction. Further, Indian law enforcement authorities must have access to that data when they need to, for conducting criminal investigations.

As in the bill's previous iteration, the Indian government has the power to notify any data as "critical personal data," which must be stored and processed only in India.

It is important to bear in mind that despite the dilution of the mandate in the Personal Data Protection Bill, all other sectoral notifications, including the RBI Payments Directive, mandating localization of payments data, continue to be in force.

Indonesia

Indonesian law has had strict data localization requirements since 2012. Government Directive 82 of 2012 mandated that all electronic system operators who provide "public services" must establish a data center in Indonesia. Seven years later, in October 2019, through Regulation 71 of 2019, Indonesia relaxed the data localization requirement by limiting the application to "public electronic system operators" – limited to the following entities: public bodies (central or regional executive, legislatures, judicial, and any other body set up pursuant to a statute), and entities that are operating electronic systems on their behalf. Crucially, public bodies operating in the banking and financial sectors are exempted from the mandate. Further, providing greater flexibility, public bodies or operators appointed on their behalf may store and process data abroad if the government decides that the "specific data storage technology" is not available in Indonesia.

Vietnam

Vietnam's Law on Cybersecurity came into effect on January 1, 2019 amid concerns that companies with an economic presence and business interest but no physical presence would also come within the ambit of this law. Article 26 (3) requires "domestic and overseas providers of telecommunications services, internet services and value added services in Vietnam's cyberspace that collect, analyze or process private information…of their service users in Vietnam" to retain data for the requisite period of time as provided by the Vietnam government. The same provision also requires that all foreign companies set up a branch or representative office in Vietnam.

After the decree was notified, there was a lack of clarity on the type of companies that would be covered by this mandate. Further unease cropped up when a draft guiding decree identified services in "cyberspace" as including all services, telecommunications, data storage and sharing, domain name, e-commerce, online payment, payments, transport networking, social networking and social media, online gambling, and providers of other services such as messages, voice calls, video calls, emails, and online games. As per a recent report by Business Times, the Ministry of Public Security greatly narrowed the width of the localization provision and stated that a

company would need to meet all of the following conditions for it to be brought under the mandate:

> (1) The company provides services on telecommunication networks, the internet or otherwise any cyberspace;AND
>
> (2) The company collects, exploits, analyzes or processes data on personal information, data generated by service users in Vietnam or data on relationships of service users in Vietnam AND
>
> (3) The company has been notified that its services have been used to commit violations of Vietnamese law but the company (i) has not taken measures to stop or handle the violations and (ii) resists, obstructs, or fails to comply with requests of the relevant authorities in cooperating to investigate and handle such violations or (iii) neutralizes and disables the effect of cybersecurity protection measures taken by the authorities.

While the first two criteria are fairly generic, the mandatory fulfilment of the last criteria greatly narrows down the number of companies that fall within the scope of the localization mandate. Only if the company has been notified that it is committing violations of various aspects of Vietnamese law and not taken remedial steps can it be forced to comply with the localization mandate, which acts as a reprieve for many global technology companies operating in Vietnam.

The Geopolitics of Data Localization

The protagonists of the data localization saga in all countries have been similar and the tussle has proceeded along similar lines. In India, the main endorsers of data localization were large Indian corporations, like Reliance or Phone Pe, that had the capacity to build data centers in India or have the financial resources to pay for the data to be stored in India.

Mukesh Ambani, chairman of Reliance Industries, has been a vocal proponent of data localization, arguing that it was a means of preventing “data colonization” by technology companies from the West, who derive rabid economic profits from the data generated by Indian citizens.

The second major force behind data localization were Chinese technology companies like Alibaba and Xilinx that had already set up data centers in India and thereby considered data localization as an opportunity to compete in India with Western companies like Amazon that had not done so.

Key proponents of data localization in Indonesia were Indonesian data center enterprises. In a joint press release dated November 2018, a number of trade organizations including the Indonesian Cloud Computing Association (ACCI) and the Association of Indonesian Internet Service Providers (APJII) voiced strong opposition to the relaxation on localization norms to little avail as the Indonesian government went ahead with issuing General Regulation 71 of 2019 regardless.

Notwithstanding domestic pressure in support, the public policy verticals of Big Tech engaged in protracted lobbying against data localization mandates in all three countries.

With respect to India, Facebook Public Policy Vice President Nick Clegg and Google CEO Sundar Pichai constantly opposed data localization and made trips to New Delhi to underscore that message. Industry lobbying groups, including the U.S.-India Strategic Partnership Forum (USISPF), U.S.-India Business Council (USIBC), and the National Association of Software and

Service Companies (NASSCOM) that represent their interests enabled these groups to provide a united front. The industry-wide lobbying efforts also linked up with the government, which made data localization a crucial talking point in U.S.-India trade negotiation, with U.S. Commerce Secretary Wilbur Ross continuously flagging it as a provision that will unduly harm U.S. companies. Secretary of State Mike Pompeo reportedly mulled restricting H1B visas for any country that has a data localization requirement and President Donald Trump explicitly opposed data localization in a statement made at the sidelines of the G-20 summit in Osaka.

The trade diplomacy and industry lobby also collaborated with card networks like Visa and Mastercard to convince the Indonesian government to loosen localization rules for its domestic payment systems. Over 200 emails uncovered by Reuters under a U.S. Freedom of Information Act (FOIA) request showed that Mastercard lobbied the United States Trade Representative (USTR) to oppose new rules on local payment systems in India, Vietnam, Laos, Ukraine, and Ghana, with Visa being roped into many of the discussions.

Google and Facebook also lobbied the Vietnamese government by speaking through their regional lobbying group, the Asia Internet Coalition, which argued that the localization requirement would stifle investment and harm economic growth.

While the Big Tech lobby and trade diplomats were clearly important figures in all three countries, they were by no means the only players in the game. Other stakeholders benefited from this geopolitical battle. Smaller start-ups in India who would have faced major economic problems due to localization related compliance costs certainly have things easier. While civil society and academia in all three countries had spoken out against onerous data localization requirements, it was finally the corporate lobby that influenced the governments into taking geostrategically sound discussions.

The Future of Multilateral Data Governance Debates

Despite narrowing localization requirements in response to the global industrial lobby and diplomatic relations, none of the three countries have compromised on their strategic autonomy. The relaxed provisions continue to provide the governments of all three countries the power to step in whenever a foreign internet service provider is not complying with the law or not providing access to data when needed and thereby, preserve sovereign interest.

The multilateral debate on the free flow of data had reached the G-20 last July with the BRICS countries releasing a strong statement emphasising the sovereign right of nations to use data for improving citizen welfare while Trump made a statement explicitly opposing data localization. Japanese Prime Minister Shinzo Abe championed the Osaka Declaration on Digital Economy promoting “data free flow with trust.” While the declaration, known as the “Osaka Track” received signatures from over 50 countries – including Brazil, China, and Vietnam – India notably refrained from signing on as they felt that plurilateral negotiations outside the World Trade Organization (WTO) would undermine multilateral fora looking to foster consensus on cross-border data transfers.

Extending India’s battle at the WTO to guarantee more sovereign control on data flows, India initially blocked the e-commerce chapter of the Regional Comprehensive Economic Partnership (RCEP) due to its obligation on the free flow of data. However, ultimately India relented and allowed for this chapter to go through. The reason provided for ultimately walking out of the RCEP was a lack of safeguards that could mitigate import surges from various RCEP countries,

especially China. This shows a willingness on India's part to compromise on its stance on the debate, if it deems this to be in its larger geoeconomic interest. Despite the data localization provisions in their law, Vietnam and Indonesia did not object to the e-commerce chapter of the RCEP, and went ahead with signing the trade agreement.

It is clear that U.S.-based technology companies will continue to shape the geoeconomic trajectory of data governance, and thus play a key role in the trade, investment, and diplomatic landscape in Asia. So long as the Big Tech lobby works closely in consultation with the governments of emerging economies to respect sovereign autonomy and promote citizen welfare over rabid corporate greed, it will continue to be a key stakeholder in shaping a free, fair, and equitable digital future.

The Author

Arindrajit Basu is a Research Manager at the Centre for Internet & Society, India. A lawyer by training, he holds a LLM in Public International Law from the University of Cambridge.