THE INDIA FORUM
A JOURNAL-MAGAZINE ON CONTEMPORARY ISSUES

July 31, 2019

Data Localisation: Mercantilism in a Networked World

By: Ashok K Nag

The deep insecurity of nation-states in a networked world makes governments demand that internet data be retained in the country where it is generated. India's approach is in line with this approach but the idea of "data sovereignty" is meaningless today.

The mercantilist school of thought that dominated the political economy of western countries between the 16th and 18th centuries is witnessing a revival. Although the economists of the time, Adam Smith and David Ricardo, convincingly argued that international free trade was to the benefit of all countries and it was not a zero-sum game as the mercantilists claimed, protectionist trade policies are finding a new acceptance with policy-makers, especially in the world's largest economy.

As the Internet virtually integrates the entire world, the creation of national boundaries around the free-flow of information in the name of national interest seems like the application of the idea of mercantilism to the digital world. India's data localisation policy should be considered an example of such "digital mercantilism".

Data is considered the most valuable asset of the 21st century. Today the companies with the largest market capitalization in the world are those that are primarily engaged in data crunching. The businesses of Google, Uber and Amazon would come to a standstill if they could not access, process, and analyse data across time and geographies.

Once nation-states realise that the most valuable assets of their citizens and territories are freely available for commercial exploitation, a clamour for protection of these assets naturally arises. As individual citizens are rightful owners of their "personal data", its exploitation without the consent of a person is a serious infringement of the privacy of that person.

The European Union (EU) has been in the forefront of creating a stringent legislative framework to protect the "personal data" of its "data subjects". The EU's General Data Protection Regulation (GDPR) is the most comprehensive regulation enacted so far anywhere. But the requirement of privacy protection does not necessarily mean that all data originating within a nation's jurisdiction are to be considered national assets. If "data subjects" were given national tags, nation-states would then consider it within their right to create barriers to cross-border data flow. The recent "data localisation" policy of various Indian regulators needs to be analysed from this perspective.

> Data localisation, in essence, is a negation of the architectural construct of the Internet.

The term data localisation is meaningful and relevant mainly in regard to data flow over the Internet. The Internet itself is a network of computing devices without any single point of failure and a consequent enabling of universal communication capability between all nodes. The Internet service providers (ISPs) are not expected to control and be aware of what data flows through the Internet. Data localisation, in essence, is a negation of the architectural construct of the Internet. There are two forms of data localisation. The first one localises storage of data. It means that ISPs must store data originating in a nation-state within the territorial boundaries of that nation-state. The second form of data localisation policy stipulates that routing of data packets must be confined within the country-specific network. This form of localisation is also called localised data routing. This is the most restrictive form of localisation. Countries adopting data localisation usually adopt the first form. Chander and Le (2015) have identified following variants of this form of localisation policy:

- preventing information from being sent outside the country
- rules requiring prior consent of the data subject before information is transmitted across national borders
- rules requiring copies of information to be stored domestically
- a tax on the export of data

Many countries are adopting data localisation policies because of their concern about the disproportionate capability of the United States (US) to access their data on national security. Such data are available on data stores of ISPs, many of which are located outside the

national boundaries of these countries. The Snowden episode confirmed the existence of a nexus, probably forced, between the US security establishment and technology firms including Google and Yahoo, allowing access to data held by the ISPs. Subsequent to the Snowden revelations, the German Interior Minister declared that, "whoever fears their communication is being intercepted in any way should use services that don't go through American servers." Ministers of France and Brazil unequivocally lent their support to data localisation policies.

It is beyond doubt that one of the important factors driving the data localisation policies of non-US countries is their desire to minimise "their comparative disadvantage in Internet data hosting" vis-à-vis US and "their comparative disadvantage in Internet signals intelligence"(Selby 2017). Thus, the data localisation policy is being adopted by countries cutting across political regimes as a comprehensive review by Chander and Le shows. The 14 countries studied by them, including India, are Australia, Brazil, Canada, EU, France, China, Germany, Indonesia, Malaysia, Nigeria, Russia, South Korea and Vietnam.

While the concerns of national governments are legitimate and require to be addressed by the proponents of an open and neutral Internet, a more informed analysis is required to evaluate the costs and benefits of a data localisation policy. It must be stated to the credit of the US technology giants that they are more eager to uphold the sanctity of the Internet than succumb to the narrow national interest of US governments. For example, Microsoft, Google, Apple, Facebook and other technology firms successfully fought the US government in court "to gain legal authority to provide the public greater detail on the information the U.S. government collects from them" (Hill 2014). Many companies are taking steps to diversify their data centre locations to escape the stranglehold of US intelligence agencies.

> This diminishing effect of a sovereign's authority over data of their citizens is the driving factor of the data localisation policies of different countries.

Tying data to territorial boundaries, also termed "Data Sovereignty", is a natural extension of the concept of sovereignty to the virtual world. Sovereignty connotes supreme authority *within a territory*. The term authority refers to, in the words of the philosopher R.P. Wolff, "the right to command and correlatively the right to be obeyed". In a modern democracy, this authority is derived from a set of principles, objectives, practices and codes of conduct called the Constitution. Data Sovereignty means that this supreme authority can be enforced on data originating within the territory and/or pertaining to the people subjected to this authority. But despite their best efforts, the modern nation states have not been able to quarantine their national data in their entirety. This diminishing effect of a sovereign's authority over data of their citizens is the driving factor of the data localisation policies of different countries.

Even a country specific domain name like www.abc.co.in does not indicate the physical location of the server which hosts the website and provides information or services. Thus the Internet is indifferent to the physical location of computing devices that comprise cyberspace. So defining Data Sovereignty in terms of territorial authority is a non-sequitur.

Recognising the futility of transcribing laws enacted for and bounded by physical space to cyberspace, Johnson and Post have called for "distinct laws" for this virtual space. For example, how do we apply anti-trust or anti-monopoly laws to companies that operate only on cyberspace? The landline based telecom companies fought to restrict internet-based voice calls (VoIP) but failed miserably.

Digital currencies are being resisted by all central banks, but there is no doubt that in the long run the central banks have to fall in line and adopt some form of a central bank digital currency. The applicability or otherwise of country-specific copyright laws to the cyberspace is another example of the distinctive nature of cyberspace. A subscription-based access to copyrighted content on the Internet has materially changed the consumers of these contents and its producers, resulting in a significant benefit to consumers in terms of reduced cost.

The Internet works on routing of messages. This works on identification of domain names and the resolution of an address within a domain. Today there are about 330 million domains. Even if a sovereign authority blocks access to some domains, new domains can be created within no time to bypass such blocking.

> The hypothesis that data localisation would prevent a foreign government from snooping on sensitive personal data of citizen of a nation-state is not borne out by some recent cyber-attacks...

China is reported to have created the most restrictive firewall that can control access to the Internet by its citizens. This might have helped in creating some of the world's largest Internet enterprises like Baidu, Tencent and Alibaba. But it might also prove to be the greatest hurdle to China realising its dream of becoming the world's dominant superpower. It is doubtful whether the world population at large would like to share the fate of the Chinese citizen – described as "world's biggest prison for netizens."

The hypothesis that data localisation would prevent a foreign government from snooping on sensitive personal data of citizen of a nation-state is not borne out by some recent cyber-attacks, believed to have been orchestrated by foreign governments. The alleged Russian interference in the 2016 US presidential election shows that in a networked world the security of data is not enhanced by creating physical access barriers to such data.

The recent example of malware-driven data hacking of the core banking system of the Cosmos Bank of India is an example of the false assurance that location provides a guarantee that data would be secure. It has been reported that the National Security Agency (NSA) of the US has "even scaled the Great Firewall of China". Thus, data localisation does not serve its primary purpose.

From a technological point of view, data localisation is not a very efficient solution for running any cloud-based application. A massive database must be partitioned and stored in distributed databases.

Today one type of partitioning known as "sharding" is followed by most large databases. Sharding breaks down very large databases into smaller databases to enable rapid data retrieval. Even a single record can be sharded into smaller parts. Database sharding allows users to maintain very large amounts of data in less expensive commodity servers. A cloud-based application cannot scale up if it maintains large databases in one place. The cost of maintaining data can increase exponentially because such large database would require high-end computers.

RBI's Data Localisation Policy

The Reserve bank of India (RBI) in a circular issued on 6 April 2018, instructed all payment system providers "to ensure that the entire data relating to payment systems operated by them are stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message/payment instruction. For the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required".

RBI's data localisation policy is driven by its intention to get unfettered access to payments data originating in India. The RBI argues that such access is an absolute necessity for effective detection and prevention of any money laundering activity. The purported reason for requiring data storage "only in India" is that without such storage within, then in the event of a conflict with the country hosting Indian payment data of a service provider, the Indian regulator may be prevented from accessing such data.

Although such an eventuality cannot be ruled out, in today's interconnected world no country can unilaterally deny access to payment data of citizens of another country. Many countries including India now share financial and taxation data with other countries through bilateral or multilateral agreements. For example, India has signed a bilateral agreement with US tax authority to identify, document, and report accounts of US citizens held in India to comply with the US Foreign Account Tax Compliance Act known as FATCA.

The Organisation for Economic Co-operation and Development (OECD) countries are signing similar financial data sharing agreements amongst themselves and with other non-OECD countries under the Automatic Exchange of Information (AEoI) initiative of G20 countries. Obviously such sharing cannot be one-way traffic. India being a member of the G20 can direct the payment service providers to store data with such countries with which it has data sharing agreements. If such an agreement is made on a reciprocal basis, an outright denial of access to India's own payment data can only be a remote possibility. India can mandate the payment service provider to share all cross-border transactions with the RBI through a FATCA-type agreement with the host country storing Indian payment data.

As regards money-laundering and terrorist financing, India is a member of the Financial Action Task Force (FATF) and has implemented its recommendations. Data localisation is not a recommendation of this international body. Additionally a government can enter into Mutual Legal Assistance Treaties ("MLATs") with other countries to access data stored in another jurisdiction but which is needed for its own lawful investigative purposes.

Data sans Frontiers

The global effort towards data localisation by nation-states is a reflection of the deep insecurity that is afflicting them in a networked world. The realisation is yet to dawn on them that the rules of the game have changed forever with the introduction of a radically different communication and workflow management architecture – the Internet -- that encompasses the entire world.

The attraction of mercantilism to the general public is its apparent pragmatism and simplicity. It ignores the feedback effect of such a policy and the long-term consequences. This is true of the digital mercantilism that is driving the data localisation policy.

The Internet was embraced by nation-states when it appeared to be merely a new form of message transfer. How the new technology was going to undermine the basis of nation-states -- the sanctity of the national frontier – was not understood. “America First” is a vacuous concept when the most valuable US incorporated firms produce goods and services in multiple territories cutting across various national boundaries.

Let me conclude by referring to the reactions when Galileo introduced his telescope to the policy makers. A senator in the Bretolt Brecht drama “Galileo” exclaims: “The contraption lets you see too much. I'll have to tell my women they can't take baths on the roof any longer". Galileo then attacked their myopic attitude saying: "These people think they're getting a lucrative plaything, but it's a lot more than that". I am afraid that our policy makers are no better than these senators of Galileo’s time.

References:

Castro, Daniel (2013) “The False Promise of Data Nationalism”, Paper published by The Information Technology & Innovation Foundation (ITIF)

Chander, A. & Le, U. P. (2015). “Data nationalism”. *Emory Law Journal*, 64(3). Retrieved from http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf

Drake William J (2016) “Data Localization and Barriers to Transborder Data Flows: Background Paper for World Economic Forum conference” (http://www3.weforum.org/docs/Background_Paper_Forum_workshop%2009.2016.pdf)

Hill, Jonah Force (2014): “The Growth of Data Localization post Snowden: Analysis and Recommendations for US Policymakers and Industry Leaders”, Lawfare Research Paper series July 2014

Selby, John (2017): “Data localization laws: trade barriers or legitimate responses to cyber-security risks, or both?” *International Journal of Law and Information Technology*, 2017

“General Data protection Regulation”, https://eugdpr.org/

“Edward Snowden ”https://en.wikipedia.org/wiki/Edward_Snowden

“Sovereignty” https://plato.stanford.edu/entries/sovereignty/