June | 2022 Discussion Paper

CUTS International
www.cuts-international.org

Impact of Barriers on Cross-Border Data Flow on Ease of Doing Digital Business in India

Asheef Iqubbal, *Senior Research Associate, CUTS International*

Overview

Data-driven services have accelerated economic inequality within and across the country which has led to calls for restrictive measures in cross-border data flows globally.[1] However, their impact on containing inequality remains unclear. India is also deliberating moving towards data localisation, an idea rooted in the concept of data sovereignty[2] that puts conditions and/or restricts data flow across national boundaries and mandates data storage within the national border.[3] In multiple draft documents such as the draft E-Commerce Policy, draft Non-Personal Data Governance,[4] proposed Data Protection Bill, 2021,[5] and Reserve Bank of India (RBI) Notification on Storage of Payment System Data, the Indian government has shown a clear intent of mandating the storage of data within national boundaries. This is being done to boost the domestic digital economy and businesses, enhancing security and privacy and strengthening law enforcement mechanisms.[6]

However, restrictive measures on data flow might lead to the fragmentation of the digital ecosystem, hampering the growing realisation of a globally connected digital economy. One of the issues stemming from data localisation mandates – increasing barriers to cross-border data flow – poses a critical concern to the future of international trade and digital businesses globally as it erects borders in cyberspace. The fundamental tenet of the Internet – free, decentralised, and open network – has brought many economic benefits.

This discussion paper, under the Ease of Doing Digital Business in India study,[7] analyses the impact of restrictions on cross-border data flows on doing digital businesses by identifying bottlenecks such as an increase in compliance, regulatory uncertainty, and inadequate infrastructure for the firms operating in multiple jurisdictions. To this end, the paper recommends mechanisms for strengthening cross-border data flow with adequate security and privacy measures for policymakers, businesses, and authorities to consider.

Introduction

Technology-led economic growth has not only accelerated economic inequality within and across countries but also opened a deep fault line in terms of surveillance and law enforcement. According to United Nations Conference on Trade and Development's (UNCTAD's) report on digital economy estimates,[8] United States (US) and China hold 90 percent of the capitalisation of the top 70 digital platforms globally. Digital corporations have strongly benefited globally from accelerated digitalisation needs due to COVID-19.[9] Concerns related to the concentration of wealth, power, threats to privacy, and security are pushing nations to recalibrate their digital governance mechanisms,

particularly the flow of data across borders. By mandating storage of data within national boundaries, the strategy of governments appears to be aimed at exerting more control over the digital ecosystem, particularly restricting the influence and domination of Big Tech. Governments claim that it will help in enhancing security, law and enforcement mechanisms, employment generation, and boosting the digital economy in the country through state control over data, data flows, and digital technologies.[10]

As governments around the world are starting to recognise the value of data and its commercial use, countries are increasingly mandating regulations that restrict the flow of data across borders.[11] Restriction on cross-border data flows targets a growing range of specific data types that can be broadly categorised as data deemed "important" or "sensitive" or related to national security. The restrictions are being mandated through data localisation policies which can be described as an idea grounded in the concept of data sovereignty where restrictions are imposed on the cross-border transfer of data and are mandated to be stored within the country.[12] Data localisation can be mandated in multiple forms such as the complete prohibition of transfer of data, allowing transfer after obtaining requisite permissions, storing mirrored copies of data within national boundaries, and taxation on transfer. Policies that restrict the flow of data include blocking the transfer of data across borders, which is also known as *hard data localisation,* or putting conditions on the data flows, storage, and processing which has been termed as *soft data localisation*.[13]

Thirty-five countries had implemented 67 restrictive measures – both soft and hard – in 2017. In 2021, 62 countries have put 144 restrictions on data flowing across the border.[14] However, it remains ambiguous how the objectives of restricting cross-border data flow will be effectively met. As a consequence of these restrictive measures that intend to regulate cross-border data flows, an open, rules-based, and innovative global digital economy is facing a growing threat. An Information Technology and Innovation Foundation (ITIF) study[15] found that a one-point increase in a nation's data restrictiveness cuts its gross trade output by 7 percent and slows its productivity by 2.9 percent, and hikes downstream prices by 1.5 percent over five years. This is because many countries are enacting barriers to cross-border data flow that make transferring data across borders more expensive and time-consuming. Basically, the flow of data across borders is fundamental for decision-making in digitally-enabled business models as businesses use data to create value and maximise that value.[16]

India already has regulations under implementation and has also proposed policies that mandate degrees of restrictions on the cross-border flow of data. In multiple recent policy documents such as the draft E-Commerce Policy, draft Non-Personal Data Governance, and the proposed Data Protection Bill, 2021, the Government of India (GoI) makes it clear that India is fast moving towards restriction on cross-border data flow. Reserve Bank of India's (RBI's) Notification on Storage of Payment System Data also points in the same direction.

Key considerations for mandating and/or proposing data localisation policies are fostering better economic growth and enhancing security. However, GoI has not backed the restriction on cross-border data flow with clear evidence as to how it will strengthen security and the growth of the digital economy. Researchers have warned that it is unlikely to enhance security as the security of data is not dependent on the data storage location.[17] Instead, security of data is highly dependent on the company's security guidelines, framework used for data protection, technical capability and they are usually uniform across the globe.

Cost-benefit analysis also needs to be taken into account while formulating policies.[18] In this context, policies that restrict cross-border data flow must be evaluated on how well they are aligned with the intended aims and their implications for the digital economy. While multiple aspects of data localisation have been debated and continue to generate significant attention, the scope of this paper will be limited to its impact on doing digital business in India, particularly focusing on small and medium businesses.

The first section of the paper situates India's data localisation move in the broader global discourse as it cannot be understood in isolation. The second section of this paper provides the impact of proposed data localisation in the context of the proposed Data Protection Bill, 2021. The second section deals with RBI Notification on data storage within India and its impact on the financial sector. The third section deals with the proposed data localisation mandates under the IT Act of 2000 and its impact on digital businesses. On the basis of analysis, the final section combines recommendations relating to mechanisms to support data flows, global digital trade and data governance.

Situating India's Data Localisation Debate in Global Discourse

As of 2022, worldwide internet networks are carrying 46.6 terabytes of data per second as compared to 100 gigabytes in 1992, which means an exponential increase in the generation of personal and non-personal data.[19] Generation of huge amounts of data and their cross-border flow has heavily contributed to the growth of data-driven enterprises globally, as it allows better coordination, efficiency, and delivery of goods and services.[20] With an increasingly central role and value of data in the global economy, the debate around storing data within the national boundary has gained significant attention.[21]

As a part of this debate, in India, like any other country, multiple sets of arguments have been put forth on the grounds of economy, security, individual liberty, among others. Policymakers have argued that data localisation will boost national digital economies, enhance security, and better law enforcement mechanisms. The UNCTAD's 2021 Digital Economy Report also states there is an urgent need to adequately regulate cross-border data flow at the international level due its increasing economic value.[22]

However, data localisation poses a significant challenge such as transnational regulatory tension. For example, the idea of adequacy, adopted by the European Union in the General Data Protection Regulation (GDPR) in order to flow data outside the European nations, is increasingly being espoused by multiple countries, including India. However, there is a lack of uniformity in terms of equivalent standard restrictions, consent restrictions, no transfer rules, and mirror copy, creating a bottleneck in the seamless flow of data.[23] GDPR creates hard localisation by laying out technical standards and requirements for handling personal information gathered in its member states and strictly restricting data transfers to "unsafe" geographies. Indian proposed law mandates the physical presence of data and/or copies within the country while countries such as China and Russia mandated additional localisation requirements including reviews of source code and restrictions on cryptography. In addition, countries such as Indonesia, Malaysia, and India have proposed to put conditional requirements on the transfer of non-personal data as well.[24]

Since regulations are still evolving and expanding, it creates uncertainty among digital businesses, adding the challenges of updating their approaches. This is particularly challenging as these approaches often require reprogramming of technological specifications. Multiple countries such as

the ones in West Asia are mandating companies to build digital infrastructure in their countries. These requirements will be difficult and resource-intensive for digital business to negotiate and comply with specific guidelines for technology decisions.[25] Businesses are not only dealing with consumer privacy but also with laws in multiple jurisdictions that put the responsibility for consumer privacy even in foreign jurisdictions. Digital platforms will find it difficult to safeguard consumers' privacy in the context of data stored in different jurisdictions.[26]

Companies are still learning to negotiate with requirements such as "equivalent standards" of GDPR. For example, the recent Schrems II decision in Europe has put restrictions on third-country personal data transfers to countries that are not currently on the European Commission's adequacy list. As a result of this, multiple companies adopted Standard Contractual Clauses (SSC) rather than Safe Harbor, which was earlier used to make a case for an adequate level of protection. The Court of Justice of the European Union (CJEU) ruled that the 'EU-US Privacy Shield' does not provide adequate protection, therefore, is no longer valid for transferring data from the EU to the United States of America (USA). This is because the USA laws do not provide data subjects 'actionable rights before the courts against its authorities'. The CJEU ruled that SSC remains valid, but on its own may not be enough to ensure an adequate level of protection. Personal data can only be transferred if the importer and the exporter can ensure that the protection set out in the SCCs can be complied with in practice. This will also impact Indian companies providing digital services in the EU and processing data in India. India now provides a basic framework for data protection but needs to straighten proposed data protection mandates.

The data localisation debate has also been mired with its impact on digital trade in terms of how it will be enforced and its impact on trade agreements. The debate around data-driven economic growth has furthered the realisation of global interdependencies through cross-border data flow. However, this has been unequally distributed. Developing countries have not been able to gain adequate benefits from the data generated domestically due to infrastructural and technical constraints. In the absence of an optimal global alliance to maintain data-driven services, the question of data sovereignty and distribution of wealth was inevitable. The US has been at the forefront against the increasing data sovereignty approach. USA's Securities and Exchange Commission (SEC) has stated that "some countries, such as India, are considering or have passed legislation implementing data protection requirements or requiring local storage and processing of data or similar requirements that could increase the cost and complexity of delivering our (firms based in the USA) services."[27]

While the General Agreement on Trade in Services (GATS), under World Trade Organisation (WTO), does not explicitly prohibit data localisation measures, there is increasing pressure to include localisation as a trade-restrictive measure.[28] In the light of increasing data localisation, more and more countries are willing to accept the free flow of data in their regional and bilateral trade agreements. A major international initiative on data flows, the Osaka Track, was launched by heads of governments under Japan's G20 leadership in 2019.[29] 'Data free flow with trust (DFFT)' with an aim to increase trust and openness in data flows co-exist and complement each other. In parallel, 76 countries launched new negotiations on digital trade in the Joint Statement Initiative (JSI) on e-commerce. The Group of Seven's (G7's) 'G7 Digital and Technology Ministers' meeting in April 2021 also discussed cooperation on Data Free Flow with Trust.[30]

These initiatives have raised multiple concerns in developing countries as it does little to quell developing countries' economic concerns. India has taken an oppositional view on unhindered free

flow of data, which the Indian government believes fails to account for emerging economies' developmental interests. At international forums, India has been a vocal critic of free flow of data across the borders due to its assertion as a developing country and stated priorities of developing policy by taking into account domestic concerns and interests. Subsequently, India did not participate in the Osaka track for DFFT and WTO negotiation on e-commerce and is even hesitant to accept it due to its apprehensions about unequal treatment of data.[31] As India assumes the presidency of Group of Twenty (G20), developing countries and MSMEs will be hoping that their needs and concerns will be considered when discussing cross border flow of data.

Impact of Barriers On Cross-Border Data Flow on Ease Of Doing Digital Business

Box 1: Draft Data Protection Bill 2021

In India, conversation around data protection started primarily in 2017 after the Supreme Court of India declared privacy as a fundamental right protected under the Indian constitution. This was pronounced in Justice K.S. Puttaswamy v. Union of India which resulted in PDP '19. After two years of deliberation and consultation with relevant stakeholders around personal data protection, in 2021, the Joint Parliamentary Committee (JPC) tabled its report on the Personal Data Protection Bill, 2019.[32] The JPC notes that data localisation will help in enhancing security, law, and enforcement, employment generation and boost the digital economy.[33] Along with multiple substantive changes including in data localisation norms, the JPC proposed changing the name of the draft bill to Data Protection Bill, 2021 (DPB '21).

The latest draft bill repeatedly argues for making data generated in India available to Indian firms. The draft bill views it as an enabling force for homegrown digital businesses to participate in the digital economy. The JPC has suggested developing gradual data localisation, aiming to enhance security and boosting the country's digital economy grounded in national sovereignty, including developing adequate technical infrastructures, taxation of the data flow, and introducing alternate payment methods.[34] The latest draft bill categorises personal data into critical personal data (CPD) and sensitive personal data (SPD).[35] Herein, the JPC proposes to mandate that a copy of CPD and SPD stored in different jurisdictions must be brought back and stored within the country in a time-bound manner.

In addition to this, the latest draft of the bill empowers the government to expand the scope of SPD under Section 15.[36] However, CPD is yet to be defined and is left to the government for an open interpretation. The JPC states that taking SPD outside of Indian borders will require approval from the Data Protection Authority (DPA) which will be in consultation with the Central Government as well as the approval of the data principal will be required. The proposed mandates also stated that the Central Government and DPA can reject the data transfer if it is not in line with the public policy or state policy. The requirement of approval includes an intergroup scheme as well. These mechanisms are being introduced to curb the "potential misuse of the provision by individuals or organisations with mala fide intentions or by foreign entities whose actions might be inimical to the interests of the State".[37] Moreover, the JPC recommendation also mandates that SPD shall not be shared with any foreign government or agency without the approval of the Indian government to "safeguard the data of Indians and keep in view the shifting nature of international relations."[38]

Compounded with the limitations on the flow of SPD, CPD has not been allowed to be transferred outside the country, unless for a few narrow exceptions relating to emergency services or certain

entities outside India after the approval by the Central Government. This can only be done by meeting adequate requirements and if the transfer of such data does not prejudicially affect the security and strategic interest of the country.[39] After DPA and infrastructures for the data storage are established, the JPC recommends, "the Central Government must ensure that data localisation provisions under this legislation are followed in letter and spirit by all local and foreign entities and India must move towards data localisation gradually".[40]

The Indian government has repeatedly affirmed that storing data within national boundaries will boost the growth of locally grown start-ups and the data-driven economy in India. While the objectives of restricting cross-border data flow may be legitimate, it might be challenging for doing digital business in India, particularly for Micro, Small, and Medium Sized Enterprises (MSMEs). Indian MSMEs account for 6.11 percent of the country's Gross Domestic Product (GDP) and 24.63 percent of GDP from the services sector, largely driven by data. India is home to many promising smaller firms that are seeking to move beyond India's borders and restrictions on cross-border data flows might be disproportionately challenging for them.[41] Currently, many MSMEs use cloud computing to store data across national servers. Requirements of storing data within national borders will inevitably increase initial and ongoing costs for both foreign as well as domestic digital businesses.[42] This is because local data services incur significant costs in terms of infrastructure, data migration, and data storage, without enjoying the same efficiencies.[43]

For example, a study in the context of GDPR shows that storing data within national borders might increase the cost of setting up servers in a country by 30-60 percent and MSMEs may not make enough profit to afford this extra cost imposed on them.[44] Further, digital businesses require hyper-scale data centres that would ensure better access and analysis of large volumes of data which will add value to their supply chain and enhance customer experience by advancing levels of personalisation.[45] There could be multiple reasons for firms to store their data across the servers, including quality, backup in case of software failure, balancing, and data sharding.[46] Despite some significant push, India currently lacks modern data centres.[47] In order to function across national boundaries, technological firms would have to bear the costs of data storage and processing mechanisms in each jurisdiction as a capital investment and the recurring costs of building data-related infrastructure. Studies have shown that restrictions on cross-border data flow negatively impact innovation and the start-up ecosystem and their ability to participate in global business structures.[48]

Further, if India continues to move towards data localisation, there could be a response to it in terms of retaliatory measures from the world, which will negatively impact the ecosystem of the Indian digital economy. For instance, the contribution of the Information Technology-Business Process Management (IT-BPM) sector to India's GDP rose from 1.2 percent in 1998 to 10 percent in 2019, which is heavily dependent on favourable policies for cross-border data flows.[49] This growth has been achieved due to the flow of data across borders, as Indian firms work with multiple businesses that are operating in different parts of the world, and any retaliatory measures will lead to the potential breakdown of data flow. This will significantly harm the growth of the data-driven service sector in India. Notably, service sectors attract the Foreign Direct Investment (FDI) inflow, which brings associated benefits to it such as knowledge and technology. Further, digital services exports also enable opportunities for innovation and start-ups by enabling knowledge and data sharing and collaboration on research and development across all sectors.[50]

CUTS study 'Digital Trade & Data Localisation' shows the unintended consequence of data localisation on India's IT-BPM Industry under different conditions of restrictions. The conditions vary according to the restrictiveness of the measures and whether they are implemented by India, its major trading partners in retaliation, or by multiple governments. The scope and extent of data restrictiveness may plunge the digital services exports between 10 to 19 percent in India. This may translate to a shortfall of US$19-36bn in achieving the digital sector's US$1tn economic value potential in 2025. The decline in digital services export will negatively affect India's GDP by 0.18 to 0.35 percent, causing a shortfall of US$9-17bn in the US$5tn economy objective in 2025.[51] Economic implications of restrictions on cross-border data flow are not limited to a loss on a relevant country's GDP, but also spread out to a decline in exports, investment, productivity and income loss to workers.[52] In view of this, framing optimal policies for cross-border data flows would be crucial for the growth of the digital economy and associated sectors and, in turn, boost the country's GDP.

A one-size-fits-all policy for regulating cross-border data flows will make doing business for digital business difficult in general and innovation and start-up ecosystems, in particular. For instance, compliance costs are also estimated to have a significant negative impact on MSMEs.[53] While bigger firms might be able to incur such costs, it would disproportionately harm the prospects of smaller firms, widening existing gaps in the equal playing field, thus, exacerbating economic inequalities. Since larger firms will be able to afford the costs of localisation more than smaller players, some of them have been staunch supporters of the pro-localisation stance.[54] Considering, competition for India's big digital businesses stems from foreign players seeking to enter the market, localisation has the potential of eliminating these foreign players, while also imposing additional compliance costs on smaller domestic players, at least in the short run. MSMEs handle CPD, so even data localisation for just this data subset could harm Indian digital businesses.

Restrictive measures in the flow of data across national boundaries might bottleneck particularly smaller ventures to access the global consumers without developing and/or renting infrastructure to store data in multiple jurisdictions. This will limit firms' capacity to provide services abroad easily and their participation in a globalised business and commerce. In the context of EU's restriction on cross-border data flow, a study found "around 65 percent of companies would need to either redesign their products or reengineer their processes. This increases to 87 percent among companies that share data intensively."[55]

Firms are likely to find data localisation requirements difficult, to provide their services to consumers, thus increasing costs and barriers to entry. Moreover, it problematises the creation of workable data sets as they are stored in multiple unfamiliar locations, thus leading to creation of vulnerable points and increasing the fear of error, particularly in the context of data mirroring. It will be expensive and put smaller companies in a vulnerable position as they are likely to find it difficult to meet adequate requirements and resources.[56]

For instance, smaller service providers operating with limited resources may not be able to differentiate between SPD and CPD – as proposed by JPC – and be compelled to store entire personal data with themselves in India. A substantial portion of SPD is being shared by data principals (users) with different data fiduciaries (service providers) while availing of various data-driven services.[57] Examples include sharing financial data with ride-hailing apps, food delivery service providers, and e-commerce companies, among others. Because of costly requirements, many smaller businesses might not be able to mobilise resources in terms of legal and technical capabilities to manage data

effectively. Research in the context of GDPR shows that due to limited technical and legal capability, smaller firms have discontinued operations or switched to less cost-effective service providers.[58]

Furthermore, requiring business firms to develop infrastructures and update and defend data storage across multiple jurisdictions would broaden the attack surface for malicious hackers.[59] Data stored in a single server within the national border prevents the sharing of data to identify IT system vulnerabilities and help firms detect and respond to cyberattacks and would fail to update vulnerable systems being lost via phishing attacks.[60] Regardless of where the data is stored, data security depends on the service provider's technical, physical, and administrative controls, which can be either strong or weak. Data localisation will increase the data breach vulnerability. Maintaining the protocol for data security across national boundaries would not be easier for business firms, particularly training staff for the sensitive functioning of data security across multiple countries.[61]

Impact on Digital Financial Services

Box 2: RBI Data Localisation

The RBI Notification[62] mandates that all payment system providers should store payment data only in India. It includes end-to-end transaction details or any information collected, processed, or carried out as part of payment instructions. The RBI Notification allows for the processing of payment data outside India for 24 hours, however, after this deadline, all such data needs to be stored within India. This was later expanded after the National Payments Corporation of India updated its guidelines that third-party application providers such as Google Pay, and WhatsApp Payments should store all payment data in India.[63] RBI's prior approval is necessary for sharing the payment system data with overseas regulators.

All payment firms, including American Express, Master Card/Visa, PayPal, Google Pay, WhatsApp Pay, Paytm, and Phone Pe, should adhere to the RBI's data localisation rule and store data within India for supervisory purposes.[64] Foreign legs of transactions may be processed offshore and financial crime compliance systems are not expected to be in the scope of RBI mandates. Along with this, banks are expected to use panel auditing firms to confirm their approach to dealing with payment data and compliance with the notice. However, any subsequent activity such as settlement processing after payment processing, if done outside India, shall also be undertaken/performed on a near real-time basis by storing it only in India.[65]

Over the past few years, India has been witnessing ongoing digital advancements in terms of innovation, infrastructure, and growth of data-driven services. These advancements propelled cashless transactions which are further fuelled by the COVID-19 pandemic. According to the Ministry of Electronics and Information Technology (MeitY), the volume of digital payments in India has increased by 33 percent. A total of 7,422 crore digital payment transactions were recorded during FY 2021-22, up from 5,554 crore transactions seen in FY 2020-21.[66] There are a number of payment options available due to Unified Payments Interface (UPI), an open Application Programming Interface (API). Along with smaller financial service providers, major players such as Google Pay, Phone Pay, and PayPal have access to sensitive users' financial data stored across international servers. This raised critical issues regarding users' data security, privacy, and law enforcement.

Increasing data breaches and security concerns pushed RBI to undertake steps aiming to protect consumers' interests. Under the Payment and Settlement Systems Act, 2007[67], RBI issued a circular in 2018, stating that all authorised Payment System Operators (PSOs) in India will have to ensure that the data is stored only in India after the processing. This includes data related to payment sensitivity, payment credentials, transactions, end-to-end transaction details, or any information collected, processed, or carried out as part of payment instructions. RBI insisted on system providers for unfettered access for supervisory purposes to all data. Proponents of data localisation argue that it will allow governmental authorities to access customers' data more swiftly.[68] Along with the development of local data centres by the payment service companies which will help in employment generation locally, it will also increase the physical presence of these companies in India, thus making them more accountable to the Indian authorities.[69]

The move forced multinational firms to comply with data localisation norms and set up data storage in India. This also led them to carry out processes like fraud monitoring and revenue assurance which were carried out outside India.[70] However, RBI's move raised questions as it did not consult with relevant stakeholders. Such measures can lead to policies without the understanding of potential consequences in terms of ease of doing digital business in India.[71] As India's fintech ecosystem has begun its expansion outside the Indian territories, it would be critical to ensure these firms do not stand oppositional to the international norms in terms of data storage and processing. It will also help India in elevating its leadership role for creative innovations in the sector. For instance, Google wrote to the US Federal Reserve to urge the regulator to build a real-time payments architecture on the lines of India's UPI.[72]

Different types of companies seem to be affected differently by the data localisation requirements of RBI. While big financial services platforms felt the disruption, start-ups and smaller firms felt the brunt to localise their data. With limited resources, smaller ones would find data localisation norms difficult and resource-intensive to comply with due to the requirement of infrastructure and resources to manage the data which will harm competition and innovation in the sector.[73] Fintech start-ups' business models significantly rely on outsourcing technical support and cloud services to affordable service providers across borders. Because of data localisation, startups will not be allowed to select affordable cloud service providers from the global competitive standards. Along with this, storing data within the national borders will compel them to undertake product re-engineering based on intricate laws in different jurisdictions, raising technical and operational costs such as compliance. For instance, financial service provider firms have been arguing that data localisation could compromise their ability to detect fraud and money laundering in the domestic payments system.[74] Real-time fraud and money laundering detection rely on noting unusual payment patterns across jurisdictions.[75]

In the context of data localisation, it will be difficult for financial services to implement and monitor uniform policies such as risk management due to varying legal requirements in each jurisdiction.[76] Decentralised models divide management attention and the allocation of resources. To manage the risks, financial services providers require a comprehensive understanding of their consumers, therefore, routinely transferring data across locations.[77] Regulations that mandate the localisation of data make it difficult to achieve these objectives, often resulting in complexity in doing digital business. Moreover, it will increase the cost of financial services as they have to create a separate infrastructure, computing capabilities, and teams for each jurisdiction. Further, it is still not clear how storing data within the national border enhances the security of data. For instance, in an international transaction, regulators will have only access to half of the data that occurred in their jurisdiction.[78]

However, this may turn into a conflict between involved authorities and legislation, thus, raising difficulty for financial services to navigate multiple jurisdictions. Due to these resource-intensive requirements, only large financial services can function in multiple jurisdictions, harming smaller businesses, startups, and innovations.

Multinational payment systems located in India faced a major impact after the RBI's data localisation. Towards the enforcement of the notification, the RBI, through two separate orders, barred American Express and Diners Club from onboarding new customers and issuing new cards after they failed to comply with the data storage requirements.[79] Moreover, for foreign companies, such compliances are an additional cost to their existing investments in the country and make the ease of doing business complicated. WhatsApp Payments also faced regulatory blockage by the RBI for many years due to not complying with the payments data storage notification, thus affecting competition in the market, and consequently impacting innovation and quality of services.[80] Similarly, RBI's mandate of storing data within the national boundary prevented Apple from launching its digital payments service, specifically designed for Apple devices in India.[81]

In 2021, RBI also restricted Mastercard from onboarding new customers and issuing new cards.[82] However, now RBI has lifted such restriction which allows Mastercard to issue new cards to customers in India. The restriction was placed in pursuance of RBI's data localisation requirements and led to strained relations of the corporation with card issuers such as banks that relied on it.[83] Notably, many banks collaborate with Mastercard to issue debit and credit cards. For a brief period of time, the move impacted the operations of some banks in issuing debit and credit cards to new customers.[84] Major financial companies expressed their discontent with data localisation in RBI's mandates, particularly in the context of RBI's directive on payment storage.[85] For instance, the Chief executive of Visa, a financial service company based in the USA, Alfred F Kelly Jr said, "there are countries like India who have decided that one of the ways to protect data is to localise it. I don't necessarily think that is necessarily the best answer."[86]

Implications of CERT-In Rules on EoDDB

Box 3: CERT-In Data Localisation

The Indian Computer Emergency Response Team (CERT-In) issued new directions under section 70B of the parent legislation, the Information Technology Act, 2000 (IT Act) on 28 April 2022.[87] CERT-In directions mandated that all firms have to maintain logs for a rolling period of 180 days within India, effectively imposing data localisation. In addition to this, service providers will have to also maintain data related to subscribers in an accurate manner for 5 years. These data sets include subscriber names, period of hire including dates, IPs allotted and used, e-mail address along with IP and time stamp used at time of registration, the purpose of availing the services, verified address and contact numbers, and ownership pattern of subscribers. However, these directions raised concerns as a public consultation was not undertaken before publishing it.

Indian Computer Emergency Response Team (CERT-In) on April 28, 2022, under Section 70B of the Information Technology Act, 2000 ("Directions") issued directions [See Box 3]. The objectives of CERT-In directions are legitimate as it attempts to address critical issues that India has been increasingly facing—cybercrimes and compromise of data security. 1.4 million incidents in 2021 and 212,000

incidents in January and February of 2022 alone have been a matter of concern for regulators as it negatively impacts the digital business community, particularly MSMEs, as well as consumers.[88]

The average cost of a data breach in India is US$2.12mn and the average time to identify a data breach stood at 239 days and it takes 81 days to contain a data breach.[89] However, CERT-in directions have mandated requirements such as maintaining logs of all ICT systems for 180 days "within the Indian jurisdiction", effectively imposing data localisation. In addition to this, the directions also mandated that multiple service providers such as data centres, cloud, and virtual private networks will have to maintain details for 5 years.

Along with big service providers such as ExpressVPN and Surfshark, smaller firms have shown their discontent with data storage requirements within India's jurisdiction. They argued that this will impose onerous costs of data-related infrastructure and compliance burdens on doing digital in India, particularly putting MSMEs in a vulnerable position as they might not have technical capability to report incidents and resources to build capacity.[90] A Small and Medium-sized Enterprises (SME) group made a submission to MeitY and CERT-In asking for an extension on the time given to comply with the latter's Cybersecurity Directions to 300 days. The submission also seeks clarity on how CERT-In would secure the data it has collected, its data logging requirement, and so on.[91] The SME group during the consultation had claimed that the heavy costs of storing logs were prohibitive for SMEs as the cost involved is approximately USD 1000 to USD 2000 weekly for one Terabyte of data.[92] CERT-In has extended the deadline for MSMEs till September 25 to comply with its cybersecurity directions. For others, the directions became effective on June 27.[93]

Questions have been raised about the way Directions were formulated on the grounds of no open consultation to take into account feedback from all stakeholders – public, civil society, cybersecurity experts, privacy advocates, and the private sector. Multiple Virtual Private Network service providers have decided to shut down their servers in India. Both ExpressVPN and Surfshark have shut down their servers in response to the CERT-In directions.[94] Nord, Proton, Express, Surfshark, Windscribe, and Mullvad, popular VPN service providers, objected to the new rules while making it clear that they will not comply with the new directions because of a lack of technical feasibility. Industry bodies raised their concerns against the directive arguing that it will make doing digital business in India tougher. In a letter they stated, "detrimental impact on cybersecurity for organisations that operate in India, and create a disjointed approach to cybersecurity across jurisdictions, undermining the security posture of India and its allies in the QUAD countries, Europe, and beyond".[95]

Recommendations

From the above analysis, it is clear that restrictions on cross-border data flow can make doing businesses difficult for digital businesses, specially smaller ones, at a significant level. In this context, to provide for EoDDB while also addressing legitimate concerns, a few recommendations are highlighted below:

1. Encouraging Transparency

Data protection mandates should take a balanced approach between safeguarding the privacy of individuals, sovereignty and promoting a receptive environment for doing digital business. Recognising legitimate concerns would be critical in building trust and optimal data governance frameworks. In this context, instead of bringing hard data localisation norms, the Indian government

should encourage firms to improve consumer trust through greater transparency about how they manage data and support the development of global data-related standards. This can be done by adopting principles such as data minimisation, retention and minimising third party access with appropriate safeguards. Firms should also ensure transparency for consumers by using different models such as dynamic consent[96] and easy-to-use proxy[97] systems that give more control to consumers over their data.

In order to ensure data remains secure, organisations should have appropriate technological, organisational, and physical safeguards in place. In the current scenario, data localisation norms override individual preferences, rather than seeking to enable individuals to make more informed decisions by equipping people with better data literacy skills and encouraging more transparency in data processing. In addition, regulators need to define the objectives of the policies and process to achieve the same more clearly and periodically analyse their impact before taking any decisions. By seeking inputs from relevant stakeholders such as Law Enforcement Agency (LEA), consumer protection organisation, digital business firms can help to ensure a fair assessment between cost and benefits.

2. Harmonising with International Norms

As the above-discussed issues stem from new age globalisation enabled by digitally-mediated architecture, the solution should also be sought from global cooperation by strengthening data governance models. At the Group of Twenty (G20), India can pursue countries for global cooperation for data sharing in order to realise more equitable global economic growth. To this end, India should be advocating the need for establishing trust across stakeholders including developing countries, regulators, consumers, industry and LEA and should underscore implications of legal certainty for the growth of doing digital business. A coordinated dialogue about how to safeguard privacy and security, while reaping the economic and societal benefits of sharing data within and across borders, will lead to less intrusive models of data regulations. By going beyond the current design of the Osaka Track, India should bring discussion and its perspectives to global forums that will build a shared understanding around standards, costs, and the solutions available to address ideological, privacy, security and technical concerns. This will create the paths for adopting greater standards of rights-protective data protection principles and frameworks.

3. Strengthen Cross-Border Data Flows

There is a need for developing progressive global architecture for data flows. While protecting its interests, India should actively participate in global efforts of ensuring cross-border data flow. Some multilateral efforts are taking shape globally to make compliance more manageable for doing digital businesses, to reap the benefits of cross-border data flows.

For example, through Digital Economy Agreements (DEAs), Singapore, Australia and the UK attempt to address some of the risks and costs of a highly fragmented regulatory environment. Similarly, through the Digital Economy Partnership Agreement (DEPA), Australia, Chile, New Zealand, and Singapore are attempting to negotiate competing interests to ensure data flow among them. Such negotiation will not only strengthen the foundation for doing digital business but also consumers will benefit from an overarching set of global principles around a common understanding of how to regulate cross-border data flow.

India has also signed an agreement with the United Arab Emirates for cross-border data flow and agreed to negotiate with Australia on the same issue.[98] These processes need to be fast-tracked to ensure India does not harm its own digital economic growth. Similarly, apart from the Trade Policy Forum and ICT working group, India should initiate dialogue with the USA on cross-border data flow by involving government officials, LEA, and trade agencies to achieve tangible objectives such as providing a conducive environment for doing digital business in both countries, addressing security concerns and providing definitional clarity. This will be important as the USA is a major exporting country of the Indian data-driven service sector.

4. Enhancing Data Security

The government may consider improving existing and building new mechanisms to enhance cross-border requests for data related to law enforcement investigations to provide timely assistance. Clarifying Lawful Overseas Use of Data (CLOUD) Act and Mutual Legal Assistance Treaties (MLATs) have been erratic. Indian parliamentary committee report revealed that in 2021, India had 845 requests pending with various countries under these two processes.[99] Drawing upon the Parliamentary Committee on External Affairs[100], India should aim for building capacities such as training programs, standardisation of requests, resource and time commitments for the handling of data access requests from abroad to effectively utilise such mechanisms. Further, India should also negotiate with its major digital trade partners including the UK, USA and Australia for better and more effective handling of undue delays and rejected requests.

---

1 Cory, Nigel and Dascoli, Luke, 'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them', 19 July 2021, ITIF, available at https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/

2 Taylor, D., Richard, 20 September 2020, '"Data localization": The internet in the balance', Telecommunications Policy, *available at* https://www.sciencedirect.com/science/article/abs/pii/S0308596120300951

3 Report of the JPC on the Personal Data Protection Bill, 2019, 2021, Ministry of Electronics and Information Technology, *available at* http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

4 Report by the Committee of Experts on Non-Personal Data Governance Framework, 2020, Ministry of Electronics and Information Technology, *available at* https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf

5 Report of the JPC on the Personal Data Protection Bill, 2019, 2021, Ministry of Electronics and Information Technology, *available at* http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

6 Report of the JPC on the Personal Data Protection Bill, 2019, 2021, Ministry of Electronics and Information Technology, *available at* http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

7 Ease of Doing Digital Business, 2022, CUTS Centre for Competition, Investment & Economic Regulation (CUTS CCIER), available at https://cuts-ccier.org/eoddbj/; Discussion Paper on Impact of Criminalising Provisions on Ease of Doing Digital Business in India, *available at* https://cuts-ccier.org/pdf/dp-impact-of-criminalising-provisions-on-ease-of-doing-digital-business-in-india.pdf; Discussion Paper on Impact of Regulatory Uncertainty on Ease of Doing Digital Business, *available at* https://cuts-ccier.org/pdf/dp-impact_of_regulatory_uncertainty_on_ease_of_doing_digital_business.pdf; Discussion Paper on Impact of Inadequate Digital Infrastructure on Ease of Doing Digital Business in India, *available at* https://cuts-ccier.org/pdf/discussion-paper-on_impact_of_inadequate_digital_infrastructure_on_ease_of_doing_digital_business_in_india.pdf; Discussion Paper on Impact of Unnecessary Compliances Ease of Doing Digital Business in India, *available at* https://cuts-ccier.org/pdf/dp-on-impact-of-unnecessary-compliances-ease-of-doing-digital-business-in-india.pdf

8. Digital Economy Report 2021, Cross-border data flows and development: For whom the data flow', 2021, United Nation Conference on Trade and Development, *Available at* https://unctad.org/system/files/official-document/der2021_en.pdf

9 Ibid

[10] Ibid

[11] Ibid

[12] Chander, A., & Schwartz, P, 2022, 'Privacy and/or Trade', *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4038531

[13] Cory, Nigel and Dascoli, Luke, 'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them', 19 July 2021, ITIF, available at https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/

[14] Ibid

[15] Cory, Nigel and Dascoli, Luke, 'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them', 19 July 2021, ITIF, available at https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/

[16] Triplett, E. Jack, Bosworth, Barry, Productivity Measurement Issues in Services Industries: Baumol's Disease Has Been Cured, *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=789545

[17] Chander, A., & Lê, U, P. (2015). Data Nationalism. *64 Emory L. J.* 677 (2015). Retrieved from https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2

[18] Chander, A., & Schwartz, P, 2022, 'Privacy and/or Trade', *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4038531

[19] Burman, Anirudh, 14 April 2021, 'How Would Data Localization Benefit India?', Carnegie India, *available at* https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291

[20] Digital Economy Report 2021, Cross-border data flows and development: For whom the data flow', 2021, United Nation Conference on Trade and Development, *Available at* https://unctad.org/system/files/official-document/der2021_en.pdf

[21] Cross-border data flows: Designing a global architecture for growth and innovation, *available at* https://www.zurich.com/en/knowledge/topics/digital-data-and-cyber/cross-border-data-flows-designing-global-architecture-for-growth-and-innovation#:~:text=Cross%2Dborder%20data%20flows%20enable%20knowledge%20and%20data%20sharing%20and,climate%20change%20mitigation%20and%20adaptation.

[22] Digital Economy Report 2021, Cross-border data flows and development: For whom the data flow', 2021, United Nation Conference on Trade and Development, *Available at* https://unctad.org/system/files/official-document/der2021_en.pdf

[23] Chander, A., & Schwartz, P, 2022, 'Privacy and/or Trade', *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4038531

[24] Localization of data privacy regulations creates competitive opportunities, *available at* https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities

[25] Beyond Personal Data: The Cost Of Data Flow Restrictions To Eu Companies, *available at* https://www.frontier-economics.com/media/5065/beyond-personal-data_the-cost-of-data-flow-restrictions-to-eu-companies.pdf

[26] Washington Post, 07 May 2019, 'The Technology 202: Activists Turn to Facebook Shareholders in Long-Shot Bid to Oust Zuckerberg,' *available at*, 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

[27] *Ibid*

[28] The Data Localization Debate in International Trade Law, *available at* https://www.ikigailaw.com/the-data-localization-debate-in-international-trade-law/#_ftn10

[29] Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows, *available at* https://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf

[30] Collective action can spark innovation for data flows, *available at* https://www.chathamhouse.org/2021/06/collective-action-can-spark-innovation-data-flows

[31] G-20 Osaka summit: India refuses to sign declaration on free flow of data across borders, *available at* https://indianexpress.com/article/india/g-20-osaka-summit-narendra-mod-india-declaration-on-free-flow-of-data-across-borders-shinzo-abe-5805846/

[32] Report of the JPC on the Personal Data Protection Bill, 2019. (2021). Retrieved from http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf [24 February 2022].

[33] Ibid

[34] Ibid

[35] Sensitive personal data includes information which may reveal, be related to, or constitute — financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or affiliation.

[36] Report of the JPC on the Personal Data Protection Bill, 2019, 2021, Ministry of Electronics and Information Technology, *available at* http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

[37] Ibid

[38] Ibid

[39] Ibid

[40] Ibid

[41] Basu, Arindrajit., Hickok, Elonnai., & Chawla, Singh, Aditya, Singh, 19 March 2019, 'The Localisation Gambit Unpacking Policy Measures for Sovereign Control of Data in India' *available at* https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf

[42] Burman, Anirudh, 14 April 2021, 'How Would Data Localization Benefit India?', Carnegie India, *available at* https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291

[43] Burman, Anirudh, 14 April 2021, 'How Would Data Localization Benefit India?', Carnegie India, *available at* https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291

[44] Quantifying the Cost of Forced Localization, *available at* https://www.leviathansecurity.com/media/quantifying-the-cost-of-forced-localization

[45] Cloudy with a chance of data centres, *available at* https://the-ken.com/story/cloudy-with-a-chance-of-data-centres/

[46] No Data Beyond This Point! – Reducing the Risk of Cross-Border Data Transfers Through Effective Information and Data Governance, *available at* https://www.connectontech.com/no-data-beyond-this-point-reducing-the-risk-of-cross-border-data-transfers-through-effective-information-and-data-governance/

[47] How India faces Unique Data Centre Infra Challenges, *available at* https://w.media/how-india-faces-unique-data-centre-infra-challenges/

[48] Data Localisation India's Double-Edged Sword?, *available at,* https://cuts-ccier.org/pdf/data-localisation-indias-double-edged-sword.pdf

[49] Kumar, B., & Rakheja, H, 2022, 'Will the Indian IT industry sustain its growth momentum?' *available at* https://www.business-standard.com/podcast/technology/will-indian-it-industry-sustain-its-growth-momentum-122012800079_1.html

[50] Cross-border data flows: Designing a global architecture for growth and innovation, *available at* https://www.zurich.com/en/knowledge/topics/digital-data-and-cyber/cross-border-data-flows-designing-global-architecture-for-growth-and-innovation#:~:text=Cross%2Dborder%20data%20flows%20enable%20knowledge%20and%20data%20sharing%20and,climate%20change%20mitigation%20and%20adaptation.

[51] CUTS International, 'Digital Trade and Data Localization', *available at* https://cuts-ccier.org/pdf/project-brief-dtdl.pdf

[52] Bauer et al, Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localisation, Paper Series: No. 30, Global Commission on Internet Governance, available at https://www.cigionline.org/publications/tracing-economic-impact-regulations-free-flow-data-and-data-localization/#:~:text=This%20methodology%20allows%20for%20the,relatively%20intensively%20on%20data%20services

[53] CUTS International, 'Digital Trade and Data Localization', *available at* https://cuts-ccier.org/pdf/project-brief-dtdl.pdf

[54] Trading in USIndia Data Flows Prospects for Cooperation in US-India Data Policy, *available at*, https://www.atlanticcouncil.org/wp-content/uploads/2022/03/Cross_Border_Data_Flows.pdf

[55] Beyond Personal Data: The Cost Of Data Flow Restrictions To Eu Companies, *available at*, https://www.frontier-economics.com/media/5065/beyond-personal-data_the-cost-of-data-flow-restrictions-to-eu-companies.pdf

[56] The economic costs of restricting the cross-border flow of data, *available at*, https://www.kearney.com/documents/3677458/161343923/The+economic+costs+of+restricting+the+cross-border+flow+of+data.pdf/82370205-fa6b-b135-3f2b-b406c4d6159e?t=1625036783000

[57] Beyond Personal Data: The Cost Of Data Flow Restrictions To Eu Companies, *available at*, https://www.frontier-economics.com/media/5065/beyond-personal-data_the-cost-of-data-flow-restrictions-to-eu-companies.pdf

[58] The economic costs of restricting the cross-border flow of data, *available at*, https://www.kearney.com/documents/3677458/161343923/The+economic+costs+of+restricting+the+cross-border+flow+of+data.pdf/82370205-fa6b-b135-3f2b-b406c4d6159e?t=1625036783000

[59] Ibid

[60] Cory, N., Luke, D. (2021). How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them. Retrieved from https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost

[61] Chander, A., & Lê, U, P. (2015). Data Nationalism. *64 Emory L. J.* 677 (2015). Retrieved from https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2.

[62] RBI Notification on Storage of Payment System Data 2018, *available at* https://rbidocs.rbi.org.in/rdocs/notification/PDFs/153PAYMENTEC233862ECC4424893C558DB75B3E2BC.PDF

[63] Bhatia, Kalindhi, 25 September 2021, 'India: RBI's 2021 Ban On Amex And Diner's Club', *available at* https://www.mondaq.com/india/financial-services/1114668/rbi39s-2021-ban-on-amex-and-diner39s-club

[64] RBI Notification on Storage of Payment System Data 2018, *available at* https://rbidocs.rbi.org.in/rdocs/notification/PDFs/153PAYMENTEC233862ECC4424893C558DB75B3E2BC.PDF

[65] RBI Notification on Storage of Payment System Data 2018, *available at* https://rbidocs.rbi.org.in/rdocs/notification/PDFs/153PAYMENTEC233862ECC4424893C558DB75B3E2BC.PDF

[66] Live Mint, 23 March 2022, India made 7442 cr digital payments FY22 at 33% growth rate: MeitY, *available at* https://www.livemint.com/technology/tech-news/india-made-7-422-cr-digital-payments-in-fy22-at-33-growth-rate-meity-11648038672792.html

[67] RBI Notification on Storage of Payment System Data 2018, *available at* https://rbidocs.rbi.org.in/rdocs/notification/PDFs/153PAYMENTEC233862ECC4424893C558DB75B3E2BC.PDF

[68] Mehrotra, Karishma, 19 October 2019, Data localisation: why, why not, Indian Express, *available at* https://indianexpress.com/article/explained/data-localisation-rbi-guidelines-banking-why-why-not-5408177/

[69] Data Divide', 16 April 2022, Business Line, *available at* https://www.thehindubusinessline.com/opinion/editorial/india-should-continue-its-efforts-to-localise-data-notwithstanding-ustrs-protestations/article65324189.ece

[70] Data localisation in India: Significance and economic impact, *available at*, https://cio.economictimes.indiatimes.com/news/strategy-and-management/data-localisation-in-india-significance-and-economic-impact/85292096

[71] Singh, Pal, Ashok, PAL, 30 July 2021, 'RBI's Mastercard Ban: Overkill, With A Touch of Protectionism', The Quint, *available at* https://www.thequint.com/voices/opinion/rbis-mastercard-ban-regulatory-overkill-with-a-touch-of-anti-americanism#read-more#read-more

[72] Live Mint, 14 December, 2019, Google wants US Federal Reserve to follow India's UPI example and build 'FedNow', available at https://www.livemint.com/news/india/google-wants-us-federal-reserve-to-follow-india-s-upi-example-and-build-fednow-11576335813947.html

[73] IRSG Report – How the trend towards data localisation is impacting the financial services sector, *available at*, https://www.irsg.co.uk/publications/irsg-report-how-the-trend-towards-data-localisation-is-impacting-the-financial-services-sector/

[74] Data localisation may hinder credit card fraud detection: Mastercard, *available at*, https://www.expresscomputer.in/security/data-localisation-may-hinder-credit-card-fraud-detection-mastercard/34099/

[75] The Great India Data localization puzzle , *available at.* https://cio.economictimes.indiatimes.com/news/big-data/the-great-india-data-localization-puzzle/89787780

[76] IRSG Report – How the trend towards data localisation is impacting the financial services sector, *available at*, https://www.irsg.co.uk/publications/irsg-report-how-the-trend-towards-data-localisation-is-impacting-the-financial-services-sector/

[77] IRSG Report – How the trend towards data localisation is impacting the financial services sector, *available at*, https://www.irsg.co.uk/publications/irsg-report-how-the-trend-towards-data-localisation-is-impacting-the-financial-services-sector/

[78] IRSG Report – How the trend towards data localisation is impacting the financial services sector, *available at*, https://www.irsg.co.uk/publications/irsg-report-how-the-trend-towards-data-localisation-is-impacting-the-financial-services-sector/

[79] RBI restricts American Express, Diners Club from on-boarding new customers from May 1', 23 April 2021, The Hindu, *available at* RBI restricts American Express, Diners Club from on-boarding new customers from May 1 - The Hindu

[80] IRSG Report – How the trend towards data localisation is impacting the financial services sector, *available at*, https://www.irsg.co.uk/publications/irsg-report-how-the-trend-towards-data-localisation-is-impacting-the-financial-services-sector/

[81] Verma,Mimansa, 20 May 2020, 'Apple has halted card payments for its in-app subscriptions in India', Quartz India, *available at* Apple has halted card payments for its in-app subscriptions in India

[82] Explained: How RBI's restriction on Mastercard impacts banking network, existing customers', 15 July 2021, India Today, *available at* Explained: How RBI's restriction on Mastercard impacts banking network, existing customers - Business News

[83] Nair, Vishwanath, 'RBI Lifts Restrictions On Mastercard In India', 16 June 2022, Bloomberg Quint Prime, *available at* RBI Lifts Restrictions On Mastercard In India

[84] RBI lifts restrictions on Mastercard over onboarding new customers, June 17, 2022, *available at* https://www.business-standard.com/article/finance/rbi-lifts-restrictions-related-to-on-boarding-new-customers-on-mastercard-122061600884_1.html

[85] Parkin, B, How US payments groups ended up on the wrong side of India's plans, 21 August 2021, Financial Times, *available at* How US payments groups ended up on the wrong side of India's plans

[86] *Ibid*

[87] 28 April 2022, 'Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet,' Ministry of Electronics and Information Technology and Indian Computer Emergency Response Team (CERT-In), *available at* https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

[88] IBM News Room, 'IBM Report: Cost of a Data Breach Hits Record High During Pandemic', IBM, *available at* https://in.newsroom.ibm.com/IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic?lnk=hm

[89] *Ibid*

[90] SME concerns with CERT-In Directions, *available at,* https://www.medianama.com/wp-content/uploads/2022/06/Compliance-window-for-SMEs-CERT-In-directives.pdf

[91] Jain, Anushka, 'Exclusive: Small And Medium Enterprises Ask MeitY For 300 Days To Comply With CERT-IN Directions', 21 June 2022, Medianama, *available at* Exclusive: Small and Medium enterprises ask MeitY for 300 days to comply with CERT-IN directions

[92] *Ibid.*

[93] Cybersecurity directions: CERT-In extends compliance deadline for MSMEs to September 25, *available at*, https://www.moneycontrol.com/news/business/cybersecurity-directions-cert-in-extends-compliance-deadline-for-msmes-to-september-25-8746581.html

[94] Mathi, Sarvesh, 'Surfshark Shuts Down Its Indian VPN Servers After ExpressVPN. Who's Next?', 8 June 2022, Medianama, *available at* Surfshark shuts down its Indian VPN servers after ExpressVPN. Who's next?

[95] Barik, Soumyarendra, 28 May 2022, 'Cybersecurity norms may make it 'difficult' to do business in India: 11 industry bodies to CERT-In', Indian Express, *available at* https://indianexpress.com/article/business/cybersecurity-norms-may-make-it-difficult-to-do-biz-in-india-11-industry-bodies-to-cert-in-7940437/

[96] Dynamic Consent: a potential solution to some of the challenges of modern biomedical research, *available at* https://bmcmedethics.biomedcentral.com/articles/10.1186/s12910-016-0162-9

[97] What is a Proxy Server? How does it work?, *available at* https://www.fortinet.com/resources/cyberglossary/proxy-server

[98] Comprehensive Economic Partnership Agreement (CEPA) between India and the United Arab Emirates (UAE). Indian Ministry of Commerce and Industry, Available at https://commerce.gov.in/wp-content/uploads/2022/03/Chapter-9.pdf.

[99] Ministry Of External Affairs. India And International Law Including Extradition Treaties With Foreign Countries, Asylum Issues, International Cyber-Security And Issues Of Financial Crimes. 2021. *Available at* https://web.archive.org/web/20211203114141/http:/164.100.47.193/lsscommittee/External%20Affairs/17_External_Affairs_9.pdf

[100] Ibid

This Discussion Paper has been written by Asheef Iqubbal, Senior Research Associate, CUTS International (aql@cuts.org). The author gratefully acknowledges the contribution of Amol Kulkarni, Director (Research), Prince Gupta and Neelanjana Sharma, Senior Research Associates, CUTS International to this paper.