Data localisation in India: *Questioning the means and ends*

Rishab Bailey
Smriti Parsheera

The authors are technology policy researchers at the National Institute of Public Finance and Policy (NIPFP), New Delhi.

We thank Ajay Shah, Amba Kak, Jyoti Panday, Mansi Kedia, Mudit Kapoor and Richard Hill for comments. All errors are our own.

The subject of data localisation has garnered significant attention in recent policy debates in India. This paper classifies the arguments around data localisation into three broad categories - the *civil liberties* perspective; the *government functions* perspective and the *economic* perspective. We examine the likely costs and benefits under each of these heads and come to the conclusion that it would be premature to adopt any sweeping localisation norms in India. At the same time, India must not will away its ability to adopt such measures in future by agreeing to sweeping 'free flow of data' provisions in trade agreements. The identification of cases where narrowly-tailored localisation requirements might be an appropriate response should be done through a transparent and consultative process. Where an assessment of the overall costs and benefits justifies a case for localisation, it should be adopted in its least intrusive form.

Contents

1 Introduction

Data localisation has become a heavily debated subject in India in light of recent policy moves towards the localisation of payment sector data and personal data. Yet, this is not a debate that is entirely new, or even unique, to India. Equally, it not a debate that can be understood in isolation. Calls for localisation must be placed in the broader context of the growing economic, strategic and political relevance of the digital economy and ensuing demands for State control and "sovereignty" in this space. Demands for increased regulation are also playing out in other fields like data protection, cyber security, surveillance, digital taxation and platform regulation, with localisation often seen as a tool to assert control in these other areas. This motivates a deeper exploration of the justifications and challenges of data localisation.

The term localisation generally refers to requirements for the physical storage of data within a country's national boundaries although it is sometimes used more broadly to mean any restrictions on cross border data flows. Following this broader approach, Chander and Le (2015) define localisation to include all measures that *"encumber the transfer of data"* across national borders. Such measures can take a variety of forms, like preventing information from being sent outside the country; requirement to obtain individual consent before making the transfer; storage of a local copy of the data; and imposing taxes on data exports. Going a step further, Selby (2017) suggests that "localised data routing", being requirements that data packets exchanged between domestic users of Internet services should flow only through domestic networks, could also be seen as another category of data localisation.

Offering a useful taxonomy, Ferracane (2017) categorises restrictions on cross border data flows into two broad heads – *strict and conditional*. The former category includes requirements of local storage or processing of data or, in stricter cases, a complete ban on transferring the data abroad. In case of conditional restrictions, the transfer of the data is made subject to the satisfaction of certain conditions. These conditions may be applicable to the persons undertaking the transfer (such as, the need to obtain the individual's prior consent) or to the transferee country where the data is being sent. For instance, one of the permitted grounds for the transfer of personal data to a third country under the European General Data Protection Regulation (GDPR) is that the country should offer an *"adequate level of protection"*.[1]

In this paper we use the term data localisation or just localisation to mean mandat-

[1] Article 45, Regulation (EU) 2016/679 (General Data Protection Regulation).

ory requirements of local storage of data. This could be in the form of exclusive retention norms, which mandate that the data should be retained *only on* domestic servers, or the slightly less stringent version of *data mirroring* that compels at least one copy of the data to be stored locally. There are of course many instances where entities could voluntarily choose to host their data locally, including for convenience or efficiency reasons (Komaitis, 2017).[2] Our focus here is only on data localisation that is compelled by laws or policies adopted by governments.

While much of the current discussion is around the economic costs and benefits of localisation, we adopt a broader approach by classifying the arguments around data localisation into three main categories. The first, is a *civil liberties* perspective that relates to the impact of data localisation on ensuring better outcomes for individuals in terms of safety of their personal data, protection from surveillance (domestic or foreign) and exercise of free speech rights. The second is a *government functions* perspective that stems from the challenges faced by government bodies in accessing data for the discharge of their enforcement and regulatory functions, including preserving national security interests. The third is an *economic development* perspective of using localisation as a lever for promoting the domestic industry. This involves an assessment of the costs and benefits of localisation measures for users, businesses and the economy as a whole.

On the first issue we point to the fallacies in the assumption that data localisation will necessarily lead to better privacy protections. Indeed the degree of protection afforded to the data will depend on the effectiveness of its data protection regime, a parameter on which India has so far been lacking. Without such protections, using privacy/security of data or the possibility of a data breach as an explanation to mandate localisation appears far-fetched or, at best, premature. Moreover, in the absence of adequate checks and balances in the law, localisation can enable intrusive information gathering by intelligence and law enforcement agencies. There is also the question of how data localisation requirements will be monitored and enforced and what this may mean from a civil liberties perspective.

Further, the claim that localisation will offer a sufficient check against unauthorised access by foreign surveillance agencies also stands to question given what we know about the pervasive and sophisticated nature of such intelligence tactics. To fully safeguard domestic data against any such interference will require a level of isolation from the Internet, which is not desirable or even possible in a modern democratic setup. That said, localisation may enable the domestic legal framework to be enforced more readily.

[2]Komaitis (2017) gives the example of applications like health monitors or autonomous vehicles that require immediate data access and response time.

Finally, to the extent that localisation measures infringe on the autonomy of individuals in respect of their personal information, the measures would have to satisfy the tests laid down by the judges in Puttaswamy v. Union of India (2017), namely, being fair, just and reasonable, having a lawful purpose, legitimate aim and amounting to a proportionate response. If it comes to such a challenge the state may struggle to justify why other measures like contractual conditions and adequacy tests for the jurisdiction of transfer did not constitute a more proportionate response than mandatory localisation. Moving beyond the realm of privacy, data localisation mandates also have a bearing on other civil liberties. Prominent among these are issues of free speech, censorship, and the right to carry on any trade or business, subject only to reasonable restrictions.

The second issue of access to data by state agencies in order to perform their functions is a compelling concern, given the acknowledged challenges in accessing evidence housed in other jurisdictions. However, even in this case we do not have sufficient evidence to suggest that mandatory localisation is a proportionate (or even adequate) response to the issue. Other solutions that have been suggested for this include fixing the broken processes under mutual legal assistance treaties (MLATs) and other bilateral or multilateral arrangements for the exchange of data between states for legitimate purposes. One may also consider the use of executive arrangements permitted under instruments such as the CLOUD Act to secure access to data held by American companies, although this comes with its own set of challenges. Moreover, to the extent that law enforcement or other regulatory agencies can identify the specific problems being faced by them in accessing particular types of data (which may be held by communication providers, intermediaries or regulated agencies) more targeted interventions involving those particular entities can be considered instead of making that a ground for bringing sweeping localisation norms.

Finally, we turn to the issue of costs and expected economic benefits of data localisation. As with any other compliance requirement, a mandate to localise data will impose significant compliance and other costs on businesses, consumers and the economy. Businesses will have to redesign their systems, bear the cost of higher data storage charges and face the challenge of storing their data in a relatively less secure environment, the costs of which will ultimately trickle down to their users. Yet, this cost, on its own, cannot be the sole basis for resisting a legal obligation. Further, given that many of the costs of localisation appear to be short to medium term in nature, could it be argued that localisation will provide benefits to the domestic economy in the long term? Unfortunately, the current state of knowledge in this field is too limited to inform sound policy decisions. While there are some studies that point to the significant macro-economic costs of localisation,

much more analysis is needed to gauge the effects of localisation at a macro as well as firm level – particularly in the context of developing countries. Ultimately, what we need is a methodical approach for judging whether the likely costs are proportionate to the benefit that is expected to be achieved in a particular context. To the extent that some of the expected benefits of localisation can also be realised through other less onerous requirements, such as, contractual commitments for the protection of data and transparent international arrangements for cross-border exchange of data, it becomes harder to justify rigid localisation norms on these counts.

In our view, it would be premature for India (and many other countries) to either opt for sweeping national data localisation laws or completely will away their ability to do so by adopting sweeping 'free flow of data' provisions that are being proposed in trade negotiations.

Against this background, Chapter 2 provides an overview of the current debates surrounding data localisation in India and broader developments in the global context. In Chapters 3, 4 and 5 we explore each of the perspectives referred to above, namely the civil liberties perspective, the government functions perspective and the economic perspective, examining the pros and cons of the arguments that are generally forwarded in each context. Chapter 6 concludes with our recommendation on the need for developing a sharper toolkit for assessing the suitability of data localisation as a proportionate response in any given context. This will require a careful assessment of the specific problem that is sought to be addressed followed a transparent evaluation of the expected costs and benefits of using data localisation as a tool to address it.

2 Current debates in India and globally

Over the past few months localisation has become a heavily debated subject in India on account of four important developments. The first was the issuance of the draft Digital Information Security in Healthcare Act, 2018 (DISHA) published by the Government of India on 21 March 2018, which seeks to empower the proposed National Electronic Health Authority to impose localisation requirements with respect to digital health data. The draft statute itself, however, does not mandate localisation of data. Next, the Reserve Bank of India (RBI) issued a directive on 6 April, 2018 imposing stringent data localisation requirements on all players in the Indian payments ecosystem. The directive, simply put, requires all payment system providers and their suppliers and intermediaries to store the entire data related to payment transactions *only in* India. The requirement also extends to

the intermediaries and third party vendors contracted to handle data on behalf of payment operators. An exception is provided for transactions that have a cross border element – the data pertaining to the foreign leg of the transaction is permitted to be stored outside the country, if required. Operators were given about six months to ensure compliance with the norms, which came into effect on 15 October.[3]

The third development was the release of the recommendations of an expert committee headed by former Supreme Court judge, Justice B.N Srikrishna that was tasked with the responsibility of proposing a new data protection framework for India (Srikrishna Committee, 2018). The Srikrishna Committee submitted its report and a draft Personal Data Protection Bill, 2018 to the government on July 27, 2018, with certain key recommendations on the localisation of personal data. Proposing a 'three-pronged model', the Committee suggested that at least one live, serving copy of all personal data should be stored in India. In addition, certain categories of 'critical personal data',[4] to be notified by the government, would be bound by a stricter requirement of being stored and processed only in India. Finally, the government would have the power to exempt particular countries, sectors or international organisation from the restrictions on free flow of data across borders on the grounds of 'necessity' or 'strategic interests of the state'.[5]

Section 97(7) of the draft Bill empowers the government to notify the provisions pertaining to cross border data flows at a time of its choosing. This implies that the said provisions may be brought into force at a different time to the rest of the statute, or indeed need not be brought into force at all. The government is currently in the process of considering these recommendations and the public comments that were invited by it on the Committee's draft Bill.

Shortly after the release of the Srikrishna Committee's recommendations, reports about a draft e-commerce policy prepared by an inter-ministerial task force set up by the government also came to light, marking the fourth important development in this debate. The leaked version of the report refers to certain categories of data being required to be stored exclusively in India (e-Commerce Task Force,

[3]A few days before the directive came into effect it was reported that 64 of the 80 payment service providers affected by the requirement had already implemented the norms while the remaining operators, including large card companies, were still in the process of doing so (Hetavkar, 2018).

[4]The Srikrishna Committee's report and draft Bill indicate that this will be a sub-category of 'sensitive personal data', which as per Section 3(35) of the draft bill, includes passwords, financial data, health data, sexual orientation, biometric data, caste or tribe, religious or political affiliation.

[5]Two members of the ten member committee have expressed their differences with the localisation mandate in the Report and have submitted dissent notes to this effect.

2018). This would include community data collected by Internet of things (IoT) devices in the public space and data generated by users in India from various sources including e-commerce platforms, social media and search engines. The document also goes on to suggest that the industry would be allowed a period of about two years to adjust to the localisation norms. The steps taken to develop capacity in this respect would include according 'infrastructure status' to data centres, improvements in power supply and connectivity and provisions of tax and customs benefits.[6] Collectively, these developments signal a clear push towards the adoption of data localisation norms across various sectors, a move that has come to be heavily criticised by stakeholders in the industry, academia, researchers and civil society groups.

2.1 Existing requirements in India

Despite the increased attention that it has garnered in recent months, the localisation question is not entirely new and, as discussed in the following section, is also not unique to India. In 2014, the National Security Council was reportedly considering a proposal that all data generated within India should be hosted in India-based servers and hence be subject to Indian laws (Thomas, 2014). While a sweeping requirement of this nature has so far not been brought into effect, context-specific localisation norms already exist in several laws and policies.

1. *Data protection under the IT Act, 2000* – At present, data protection provisions in Indian law are contained primarily in the Information Technology Act, 2000 (IT Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (IT Rules). Section 43A of the IT Act provides for the payment of compensation for failing to maintain reasonable security practices in respect of sensitive personal data. The IT Rules issued in 2011 clarified the meaning of sensitive personal data and set out the norms for the collection, disclosure, storage and security of such information.

   The IT Rules permit a body corporate to transfer sensitive personal data to another entity or person (in India or elsewhere) upon ensuring that the other person will be able to provide that same level of data protection that is expected under the IT Rules. Further, the transfer is allowed only if necessary for the performance of a lawful contract or if the person has consented

[6]Reports appearing in the media immediately prior to publication of this paper indicate that the government may reconsider the policy, though it is still unclear what has prompted this reversal or whether localisation norms will make a re-appearance in any future drafts of the e-commerce policy (Bhan, 2018).

to data transfer.[7] Soon after the release of the rules the government issued a clarification that the rules were only applicable to body corporate or person located within India (Ministry of Communications, 2011). While laying down these requirements the law does not establish any process or substantive standards to determine when an entity may be in a position to provide the "same level of data protection" (Sinha & Hickok, 2018). In general, the enforcement of these requirements, and as a result, compliance with them, has remained questionable.

2. *Government data* – The Public Records Act, 1993 prohibits the transfer of public records out of Indian territory without the prior approval of the Central Government unless such transfer is being made for an official purpose. The government's "MeghRaj" initiative, which is designed to promote the use of cloud services by the government, also contains a requirement for the localisation of government data. The conditions for empanelment of cloud service providers under the initiative require that *"data center facilities and the physical and virtual hardware should be located within India"* (DeITY, 2015).

   The National Data Sharing and Access Policy (NDSAP) notified by the Ministry of Science and Technology in 2012 presents yet another instrument for mandating localisation requirements for government related data. The NDSAP provides for the sharing of all non-sensitive data that is generated using public funds by different ministries, departments and agencies of the Government of India. Therefore, current laws and policies already provide for full data localisation in so far as government records and publicly funded data from government sources is concerned.

3. *Sector-specific requirements* – In addition, certain sectors-specific localisation requirements are also applicable. For instance, the security conditions in the license agreement entered into between telecom service providers and the government bar the licensee from transferring any user information or accounting information relating to a subscriber to any person/place outside India. Exceptions are provided for situations where such information may need to be transferred for international roaming or billing purposes.[8] Compared to this, the rules notified by the Ministry of Corporate Affairs for maintenance of accounting records by companies contain a relatively less stringent requirement of maintaining a local copy. As per the Companies (Accounts) Rules, 2014, the back-up of the books of account and other books and papers of the company maintained in electronic mode, including

[7] Rule 7 of the IT Rules.
[8] Clause 39.23(viii), Chapter VI (Security Conditions) (Unified License, 2014).

at a place outside India, should be kept in servers physically located in India on a periodic basis.[9]

2.2 A closer look at RBI's payment directive

A closer look at the process (or lack thereof) behind the RBI's localisation Directive can offer some valuable lessons for future policymaking on this subject, whether in terms of the sweeping requirements proposed by the Srikrishna Committee or on a sector by sector basis. The RBI's directive was notified without any prior notice or public consultation and with little explanation on the motivations for this decision. Yet, this sort of conduct is not out of the ordinary for many decisions that we see in the Indian financial sector. This is despite repeated acknowledgements from the government and financial sector regulators about the need for improvements in regulatory processes.

In 2013, the recommendations of the Financial Sector Legislative Reforms Commission (FSLRC), an expert body set up by the Ministry of Finance, had led to the publication of a handbook by the Ministry noting that the drafts of all subordinate legislations should be published before they come into effect, along with a statement of objectives, explanation of the problem to be addressed and an assessment of potential costs and benefits. This followed from a decision made in a meeting of the Financial Stability and Development Council (involving all financial sector regulators) to adopt better regulatory governance and transparency practices in framing regulatory interventions (FSDC, 2013).[10] However, not much has changed in practice.

Had the RBI followed a more open and rigorous process in this case we might have had more clarity about whether the initiation of this particular intervention was preceded by an articulation of a specific problem that needed to be addressed. The RBI notes in the Directive that its objective was to ensure unfettered supervisory access to payments data for monitoring purposes. Further, RBI's Statement on Development and Regulatory Policies, which preceded the Directive, also referred to the need for adopting the best global standards in safety and security of data to reduce risks of data breaches. Barring these broad references, there is no mention of the specific challenges that were being faced by the RBI in accessing payments data under the existing system.

Were there instances of non-compliance to data requests by regulated entities?

[9] Rule 3(5), Chapter IX, Companies (Accounts) Rules, 2014.

[10] Similar suggestions were also made specifically for the payments sector in the report of the Watal Committee on Digital Payments (Wattal Committee, 2016).

Was the location of the data in another jurisdiction the reason for non-compliance? On the security front, were there security breaches that occurred on account of payments data being stored outside India? Were there lapses in how the security breaches were handled and were they related to the physical location of the data? In the absence of these explanations, the Directive seems to lack sufficient evidence and reasoning to support its motivations.

Even if we assume that the problem was correctly identified, the next step would be to assess whether the selected intervention would pass the *"Occam's razor of public policy"* (Ajay Shah, 2016) – does it use the least coercive tool to achieve an identified outcome? This question becomes particularly relevant given that the Payment and Settlement Systems Act, 2007 (Payments Act) already contains wide powers allowing the RBI to call for periodic information from payment system providers and gain access to their information (Sections 12 and 13). The directive is unclear as to why localisation constitutes a necessary tool to give effect to this statutory power.

Further, the Directive also does not appear to have taken into account the the fact that most financial entities maintain their data in an encrypted form. The RBI itself requires banks and other entities to utilise 128 bit encryption to secure online communications and to protect sensitive personal data while at rest. Similarly, the National Payments Corporation of India also mandates the use of encryption to store customer data. Encryption renders the data illegible without assistance from the relevant payment entity (or a significant effort being made to crack the encryption). Given that the premise behind mandatory localisation of data is to ensure unfettered supervisory access to the data, the Directive fails to consider that regulatory authorities will still have to request the payment entity to decrypt the data, in line with legal processes, before it can be accessed and used.[11] Therefore, the RBI would presumably still need to follow other processes to ensure "unfettered supervisory access" to the data, even though it may be stored in the country. This highlights the shortcoming of imposing localisation requirements without considering the broader technological environment – merely mandating localisation is unlikely to meet the stated regulatory ends.

Finally, did the RBI consider other alternatives before opting for a strict localisation mandate? Perhaps near real-time reporting requirements for certain kinds of data could have achieved the regulatory objective without micromanaging the

[11] Section 69 of the Information Technology Act, 2000 lays down the circumstances under which decryption orders can be issued by the government – in the interest of sovereignty, integrity or defence of India, security of the State, friendly relations with foreign States, public order, preventing incitement to the commission of any cognizable offence relating to the factors mentioned earlier, or investigation of an offence.

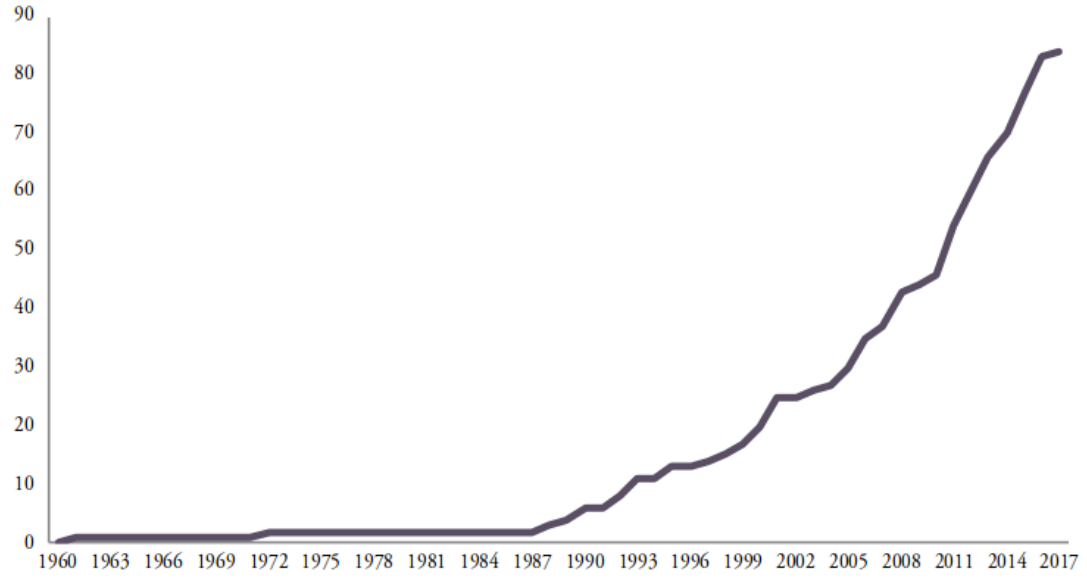
exact location of the data. Similarly, could a requirement to keep a copy of all the data in India have ensured the same level of regulatory access? Absent a transparent regulation making process we have no way of knowing the different options that were considered by the regulator, or the factors that motivated the selection of this particular option.

By not following a formal consultation process, the regulator missed the opportunity to take into account the holistic implications of its move on payment operators and the sector as a whole. Had the RBI followed such a process, which would include a cost-benefit analysis of the possible regulatory options, it is more likely to have found a way to achieve the desired objectives through less restrictive means. At the very least, the requirement to store all the data *only* in India is not likely to have found its way into the final Directive.

2.3 Tracing the global trends

The developments in India also need to be placed in the context of global localisation trends. As per the Digital Trade Estimates index created by the European Centre for International Political Economy (ECIPE), in the period from 1961 to 2016, 84 data localisation requirements were introduced in the 64 countries covered by the index (See Figure 1). Of these, 42 percent of the measures imposed certain conditions to be fulfilled before the transfer of the data; 25 percent imposed local storage (but not processing) requirements; and 33 percent imposed local processing requirements or a complete ban on transfers outside the jurisdiction (Ferracane, Lee-Makiyama, & der Marel, 2018).

Figure 1 Cumulative Number of Data Localisation Measures (1961-2016)



Source: Ferracane, Lee-Makiyama, and der Marel (2018)

While there are some countries like Russia, China, Vietnam and Indonesia that have adopted relatively broad-based localisation requirements, most others tend to apply differential standards based on the nature of the data and the sector to which it pertains. To take a few examples, sectoral localisation norms are seen in Australia (health data), France (data relating to judicial proceedings) and Germany (telecommunications metadata and tax accounting data) (Cory, 2017). It is also common to find localisation requirements being mandated for government / public sector data. A study on data localisation measures adopted by members of the European Commission also found that certain kinds of data, namely tax and accounting data, defence and security data, financial data and data held in public registries, was more commonly being subjected to localisation requirements. The extent of restrictions also varied among the Member States, with most of them having only one (8 countries) or two (7 countries) types of restrictions (EC Staff Document, 2017).

Links can be drawn between the massive surge in data localisation measures in the last ten to fifteen years and global developments in terms of the rise of the data-driven economy with accompanying social, economic and political consequences. In the absence of any global compact to maintain the Internet as a unitary structure, the assertion of territorial and sovereign claims over this space appears inevitable and has in fact been ongoing since the early days of the Internet. As noted by

Goldsmith and Wu (2006), *"the Internet has not, as some of its early users and developers would have wanted, rid itself of the abiding significance of geography"*, but has evolved and continues to evolve to take into account the different cultures and societies it interacts with. Seen in this context, data localisation fits in as one of the pieces in the broader slew of measures aimed at exerting national control over portions of the digital ecosystem.

While data localisation decisions clearly seem to fit within the mould of 'protectionist' national strategies, when it comes to publicly acknowledged reasons, most countries choose to rely on other grounds such as data protection, law enforcement and preventing foreign surveillance as the basis for their localisation decisions.[12] In this context, Kuner (2015) argues that localisation demands could genuinely stem from factors that go beyond protectionist measures. Therefore, rather than merely positing factual arguments pertaining to the benefits or harms of localisation mandates, one may be better served by locating the debate within a broader normative framework. Examples of such normative values would include *"freedom of expression, antidiscrimination, privacy as a fundamental right, and ethical considerations"*. For Kuner, such an approach would avoid presupposing the desirability of certain types of values (like economic development) at the cost of other values that may be equally or more desirable for a particular society. In the chapters that follow we outline the arguments that are typically extended to further the demands of data localisation and examine their implications from a range of different perspectives.

3 The civil liberties perspective

One of the primary characteristics of the Internet is its ability to transfer information freely across national borders. This has led to debates around the virtues of maintaining the network as a 'free space' - ostensibly free from government control (Goldsmith & Wu, 2006). The wide ranging benefits from this approach span from unrestricted innovation to enhanced civil liberties, particularly in the form of freedom of speech and expression. However, the limited ability of states to effectively regulate this space have also led to new kinds of harms and challenges to the traditional human rights framework.[13] Examples include the increased potential for

[12]Of the fourteen jurisdictions whose data localisation norms were studied by Chander and Le (2015) only two countries - Nigeria and France - explicitly recognised 'economic development' as a rationale for their localisation decisions.

[13]There are numerous efforts to update and further elucidate both global and Indian rights frameworks in the digital context. In the international context one may look, in particular, to work by various UN special agencies, special rapporteurs, as well as global civil society organisa-

public and private surveillance, online harassment, spread of misinformation and privacy violations. It has therefore become difficult to argue against the imposition of any kind of domestic regulation over the Internet in the absence of any global compact to this effect (particularly given the general recognition that offline law applies equally online) (United Nations Human Rights Council, 2012) and (United Nations Human Rights Council, 2016).

The challenge now lies in figuring the optimum tools for regulation of the Internet and the overall digital ecosystem in ways that will lead to the overall enhancement of human rights and well being. While on one hand, the state is bound to provide efficacious remedies to individuals – a need that can only be met through the application of some legal framework to the online space – on the other, there are fears of excessive regulation and increased fragmentation of the Internet through exercise of sovereign controls. A possible route to progress, as noted by the European Data Protection Supervisor, may be to ensure that all future Internet governance models are underpinned by a respect for fundamental rights (European Data Protection Supervisor, 2014).

In the context of localisation, it has been suggested that measures that are imposed specifically to enhance civil liberties protections should be viewed differently from those imposed for economic or protectionist reasons. Kuner (2015), for instance, proposes that a country may decide to "*sacrifice a certain amount of economic efficiency in exchange for promoting other legitimate values that it believes are furthered by data nationalism*". In response, however, it could be argued that deciphering the reasons for a localisation mandate is not always straightforward – governments can and do take actions for multiple reasons that may not be obvious to analysts at first glance. Even a seemingly protectionist stance can be brought within a rights discourse – for instance, by pointing to the need to preserve economic or social rights. Ensuring the protection of one person's rights over that of others, such as in case of public order, morality, etc., could be another lens of enquiry.

Therefore, rather that viewing the issue as a trade-off between civil liberties and economic development or costs, a more useful exercise would to balance competing rights – the civil liberties protected by localisation versus those harmed by it. We attempt to do so in this section by presenting the factual arguments for and against localisation from a civil liberties perspective. We focus in particular on the rights to privacy, and speech and expression, which are guaranteed as fundamental rights under Part III of the Indian Constitution.[14]

tions. See Human Rights Council (2016), LaRue (2011), Canatacci (2018), and Necessary and Proportionate (2014).

[14]Fundamental rights are inalienable rights that form part of the basic structure of the Consti-

3.1 Right to privacy

In August, 2017, the Supreme Court of India recognised that there exists a fundamental right to privacy under the Indian Constitution (Puttaswamy v. Union of India, 2017). The Court, in a wide ranging declaratory judgment, found privacy to be an integral component of numerous fundamental rights, notably rights to equality (Articles 14-18), speech and expression (Articles 19(1)(a)), and the protection of life and liberty (Article 21). While recognising that the right could have multiple facets (informational privacy, freedom from unwarranted stimuli, autonomy to take decisions, etc.), the court noted, that as with other fundamental rights, the right to privacy is not an absolute right, and can be restricted on certain overriding grounds.

The Supreme Court adopted a variety of approaches in reaching its conclusions (there were six separate opinions given by the nine judges on the bench). However, there was consensus on the point that any interference in the right to privacy should satisfy the requirement of a "fair, just and reasonable" procedure established by law. Further, the majority of judges also converged on certain additional tests to be used for analysing any privacy infringements. These tests include: the existence of a law, that the law should seek to achieve a legitimate state aim, and there should be a rational nexus between the objects and means to adopt them (proportionality) (Bhandari, Kak, Parsheera, & Rahman, 2017).

While it is still early days in India in so far as application of these tests to factual situations is concerned,[15] it is clear that to the extent that localisation measures infringe on the autonomy of individuals in respect of their personal information, the measures would have to satisfy the *Puttaswamy* tests.

In the following sections we identify three sets of issues to be considered while assessing how localisation may affect privacy rights. *First*, architectural issues based largely on differences over how centralisation or decentralisation of data may affect privacy and security of data; *second*, effects of localisation norms on foreign and domestic surveillance; and *third*, adequacy of the existing privacy framework in India and what localisation may mean for that.[16]

tution – that can not be significantly amended or abrogated. Each fundamental right is, however, subject to a specified set of reasonable restrictions.

[15]The tests and standards were applied and elucidated further in the recent judgment of the Supreme Court concerning the validity of the Aadhaar identity project (Justice KS Puttaswamy (Retd.) v. Union of India, 2017).

[16]A fourth set of concerns pertaining to the cumulative impact of physical localisation with other broader localisation norms - such as equipment purchase or import restrictions can also be considered although this is beyond the scope of how we define localisation for the purposes of this paper. By limiting access to high technology or more efficient equipment, privacy protections for

3.1.1 Architectural impact on data security

What would be the privacy and security impact of increased centralisation of information on account of mandatory localisation? One perspective is that localisation may lead to lower data protection as domestic entities may lack access to the necessary infrastructure and technical or human capacity to implement strong data security measures (compared to bigger, globally competitive entities based in jurisdictions of their choice) (Chander & Le, 2015). Kuner (2015) however points out that this fails to take into account the fact that hackers often target large global players, precisely because of their size and the quantity of user information they store (the 'jackpot' problem).

A second argument is that the forced splitting of data sets (as may be required with a mandate to localise certain types of data) can lead to the creation of more points of failure (Cohen et al., 2017). It is also argued that mirroring requirements may increase the likelihood of errors in data[17] and that the costs of localisation may lead to a reduction in the ability of entities to adequately allocate and match risks of data breach with appropriate levels of security.[18] These too, can be countered by pointing to the jackpot problem or the relative merits of decentralisation.[19]

It appears that while arguments may be made for and against the impacts of localisation on data privacy in any specific factual context, it is unclear whether mandatory localisation is always an appropriate or efficient means to achieving this end. Equally however, permitting free trans-border flows of data would not *in itself* lead to enhanced privacy protections.

Two broad principles emerge from this discussion. One, the chance of a data breach is determined more by the technical measures, skills, cyber security protocols, etc., put in place rather than the mere location of data (J. Hill, 2014). Two, there is a need for appropriate technical frameworks to be put in place to preserve privacy both locally and globally – for instance, through building in privacy by design mechanisms in networks and digital systems and encrypting user data (Sargsyan,

domestic users may be reduced (Cohen, Hall, & Wood, 2017).

[17] As more copies will need to be updated or maintained, with changes accurately reflected in each copy (Cohen et al., 2017).

[18] By having to spread their resources over a large number of locations, global corporations would logically end up reducing the security at each level, in view of the cumulative costs (Cohen et al., 2017).

[19] An interesting example of the benefits of de-centralising or mirroring data can be found in the case of the NotPetya malware attacks in Europe in early 2017. The attacks crippled businesses including that of global shipping giant Maersk, which was able to recover its internal IT systems only due to the fact that a data center in Ghana (that was unaffected by the malware attack) contained a mirrored version of its domain controller data (Greenberg, 2018).

2016).

3.1.2 Domestic and foreign surveillance

Physically locating all data within the territory of a state leads to a significant increase in the capacity of law enforcement agencies to access that information, and consequently surveil domestic residents.[20] Localisation becomes problematic in this context not just because the data will now be under the physical access of the state, but also due to the technical measures likely to be implemented to ensure that the data stays within a country's boundaries. For instance, localisation may require invasive checking of IP addresses or other types of addressing data/metadata.[21]

The increasing use of localisation measures is however linked more often with the Snowden revelations in 2013 that disclosed the pervasive nature of foreign surveillance activities.[22] This draws from the argument that while domestic surveillance can certainly be a matter for concern, foreign surveillance is arguably more problematic due to the challenges that this poses for national security, as well as the inability of the public to carry out any democratic oversight of such mechanisms (Kuner, 2015). While this argument has its merits, the effectiveness of using localisation as a counter to foreign surveillance needs to be questioned on certain counts.

First, besides the direct measures used by foreign intelligence agencies to access data through corporations situated in their own jurisdictions, reports have also indicated the extensive use of extra-territorial measures. Access to data stored on domestic networks and computer systems of numerous countries, including India was enabled through the use of tampered hardware (Greenwald, 2014); by injecting malware into systems (Gallagher & Greenwald, 2014); and securing physical access through entities operating domestically (Press Trust of India, 2014). Given the complexity of these issues, deeper thinking is needed on a variety of fronts. The solutions may, for instance, range from developing local manufacturing capacity, ensuring multiple communication channels into and out of the country, checks on import of hardware systems and other mechanisms for improving network security.

[20] See Chander and Le (2015) and J. Hill (2014). For instance, it was reported that Russian data localisation norms were to a large extent put in place due to the problems that domestic intelligence agencies had with cracking the https protocol, which was used primarily by non-Russia based websites (Nocetti, 2015).

[21] Data sets may also have to be tagged to ensure they can be identified and processed within the country or exported as appropriate, further exacerbating privacy concerns (Chander and Le (2015) and J. Hill (2014)).

[22] See Chander and Le (2015), J. Hill (2014), and Hoffman (2015).

Localisation on its own is not likely to be a sufficient barrier against sophisticated intelligence threats from abroad.

Second, in today's geo-political ecosystem, personal data can be viewed as a currency to be traded between nation states – implying that all countries have a rationale to capture as much data as possible (Sargsyan, 2016) and are often complicit in its exchange. The Snowden revelations, for instance, revealed not only the broad information sharing arrangements between the 5-eyes countries (the United States, the United Kingdom, Australia, Canada, and New Zealand) but also how numerous other countries (including India) have signed up as third party partners.[23]

Third, laws such as the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) passed by the United States permit American executive authorities access to offshore data held by American companies, (while also permitting foreign countries to enter into agreements with their American counterparts to access data held by American companies.[24].

Finally, there is the fact that citizens in countries with poor checks and balances often do not have any real or effective mechanisms to challenge state surveillance mechanisms. Additionally, domestic executive agencies will generally pose a greater threat to an individual than foreign agencies, due to the relative ease of applying coercive action within a state's boundaries. Nevertheless, one must also consider that localising data may enable the exercise of legal rights by local citizens against any form of unauthorised access to data, including by foreign intelligence agencies.

3.1.3 Adequacy of the data protection framework

The increasing privacy awareness in India, particularly after the *Puttaswamy* case and the Cambridge Analytica-Facebook incident, is often used as a peg to demand the localisation of personal data.[25] Given the variety of information shared online, and the possible harms that may occur from unauthorised disclosures, there is no doubt that we need better systems for protection of Indian data and particularly

[23]See Borger (2013) and Geist, Gjerding, Moltke, and Poitras (2014). Interestingly, India and the US are currently in the process of executing a number of agreements that could facilitate easier exchange of information for both military and civilian use. See Sehgal (2018) and George (2018).

[24]The enactment of the CLOUD Act itself is not without controversy, and the law is facing pushback from civil rights activists as well as large corporations such as Microsoft (Ruiz, 2018).

[25]Refer for example to the Justice Srikrishna Committee's analysis of the matter (Srikrishna Committee, 2018).

data of a sensitive nature. It is however questionable whether merely locating data within the territory of India would actually make it any safer or less likely to be misused, particularly till the time that we have in place a holistic and well-functioning data protection law.

While the Srikrishna Committee has published a draft Personal Data Protection Bill, 2018, the provisions in the bill do not necessarily go as far they could, particularly to safeguard against unchecked state surveillance.[26] In any event, it is unclear how long it will be before relevant legislation can be enacted in India and further, how long it will take to build the necessary institutional capacity to adequately investigate and prosecute breaches under this law. This is particularly significant as current Indian laws pertaining to surveillance provide significant leeway for the state to exercise fairly intrusive powers. It is in fact arguable that current laws pertaining to surveillance (as contained in the IT Act and Telegraph Act, 1885) do not comply with Supreme Court's dicta laid down in the *Puttaswamy* case (Bailey et al., 2018).

The existing privacy framework under the IT Act continues to be woefully inadequate, in terms of substantive protections, remedies and implementation.[27] In the circumstances, putting in place sweeping data localisation requirements without a commensurate and strong data protection regime could act to lower rather than strengthen the protection accorded to Indian data.

[26]While the draft bill proposes far greater set of protections than what is currently available, including through improved grievance redressal and punitive processes, it also has several shortcomings. The exceptions granted for instance, to the state, do not inspire confidence that the localised data will be safe from unauthorised or arbitrary use. To illustrate, Sections 13 and 19 of the draft law provide the state with wide grounds to process an individual's data. Even sensitive personal data may be processed if 'strictly necessary' for the exercise of any state function authorised by law (for the provision of a service or benefit to the data principal). More worryingly, Sections 42 and 43 of the draft law provide broad exemptions from the law for actions taken in the interests of security of the state and for the prevention/detection/prosecution, etc. of offences. The draft law therefore fails to implement many procedural or other safeguards required to protect citizens from state excesses as far as surveillance is concerned (Bailey, Bhandari, Parsheera, & Rahman, 2018).

[27]Not only are the substantive provisions of law inadequate, for example, the Indian legal framework lacks some basic protections that are part of well-developed data protection laws, such as provisions for data breach notifications, the remedies available under the law are, also limited to compensation under Section 43A and penalty for disclosures made in breach of a contract under Section 72A of IT Act.

3.2 Freedom of speech and expression

Article 19(1)(a) of the Indian Constitution protects the right to speech and expression, which may be restricted only on the grounds provided in Article 19(2).[28] Article 19(2) uses the phrase 'reasonable' to qualify the permissible scope of a restriction.This generally implies a lack of arbitrariness, vagueness or excessiveness in the measures adopted (Basu, 2012).[29] Reasonability also implies the need for a 'proximate nexus' between the harm sought to be prevented against and the restrictive measures adopted by the government (Bhatia, 2016).

The right to expression has been held to include within it the right to both disseminate and receive information.[30] Indian courts have also recognised the important role of the Internet in enabling the right to expression, notably in the Shreya Singhal v. Union of India (2015) case. Referring to the Internet as a 'marketplace of ideas', the Court observed that the Internet enables individuals to access many different points of view. Accordingly, it struck down Section 66A of the IT Act - which penalised the sending of offensive messages through computers - as being overbroad. In support, the Court cited the possible chilling effects of such a law, as well as its susceptibility to misuse (due to its vague and imprecise nature and the lack of procedural safeguards to limit its use).[31]

Applying this to the context of data localisation measures would imply that the scope of the measure may need to be narrow in view of the Internet's character as a tool to further expression rights.[32] That said, despite the general recognition of the

[28]Restrictions may be imposed on grounds of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence.

[29]Courts often give importance to the need to implement procedural guidelines to limit unfettered exercise of state power. See for instance, (People's Union of Civil Liberties (PUCL) v. Union of India, 1996).

[30](Secretary Ministry of Information and Broadcasting, Government of India v. Cricket Association of Bengal, 1995). Notably, in this case the Supreme Court has opined on the need for citizens to have access to a plurality of views on all public issues, so as to ensure an 'aware' citizenry

[31]The Court did however recognise that special offences may be created for the Internet in view of the nature of the medium and the particular problems that it may create to society. The Court also read down IT Act provisions pertaining to intermediary liability to ensure that content would only have to be taken-down through a process accessible only to law enforcement agencies and courts.

[32]In this context, it is also worth noting that the Internet has also been accorded certain special protections – notably in the form of net neutrality regulation. Both the Telecom Regulatory Authority of India (TRAI) and the Government of India have accepted the principle of network neutrality in order to preserve the openness of the Internet, and the ability of users to freely access content. By limiting the ability of service providers to create 'walled gardens', the telecom

importance of the Internet to the furtherance of civil liberties, we see a worrying trend where the government and courts often end up using blunt instruments such as blanket Internet shutdowns in the place of more targetted/proportionate measures.[33]

Localisation could affect expression rights in a number of ways given that the Internet is built on the principle of easy transfer of information across borders (Chander and Le (2015) and Plaum (2014)). It could effect access to transborder media and applications – particularly insofar as smaller content providers are concerned. To illustrate, smaller foreign platforms, while used or accessed by Indians, may not view the country as their primary market to justify the costs of complying with stringent or overbroad localisation norms.[34] Localisation may also permit greater censorship of domestic dissident or political voices and affect the extent to which Indian content is accessible abroad.[35] Moreover, besides limiting the overall generativity of the Internet, localisation can also have a negative effect on the ability of the scientific and business community to innovate with big data solutions at a global scale, and hinder innovation based on the Internet of Things and the sharing economy.[36]

While merely locating data in a country does not in itself (or automatically) make it vulnerable to censorship (or surveillance); data would certainly be more vulnerable if the country the data was located in had laws that gave the state greater powers of restricting access to content, or indeed if the country the data was located in did not have the capacity or will to ensure proper oversight and accountability of its executive agencies. The use of extra-legal measures is also more tempting should data be localised.[37]

In this context, it is useful to briefly examine the current state of Indian laws as regards censorship of the Internet. As with surveillance, the state has the power to block online content using either specific laws under the IT Act, 2000 or general

regulator recognised that *"the use of Internet should be facilitated in such a manner that it advances the free speech rights of citizens, by ensuring plurality and diversity of views, opinions, and ideas"* (TRAI, 2017), (Bhargava, 2016).

[33]See Bhatia (2017a), Bhatia (2017b) and Hariharan and Baruah (2015).

[34]There are examples to show that the the imposition of the General Data Protection Regulation in Europe earlier this year saw numerous American services – ranging from online games to newsmedia companies making themselves unavailable in Europe. See Connolly (2018) and Sentance (2018).

[35]See Chander and Le (2015) and Chander (2011).

[36]See Zittrain (1974), Ursic, Nurullaev, Cuevas, and Szulewski (2018) and Ahmed and Chander (2016).

[37]There is no real incentive for law enforcement agencies to consistently adhere to due process norms given that Indian law does not bar the introduction or use of illegally acquired evidence (State (N.C.T. Of Delhi) vs Navjot Sandhu, 2005).

laws such as the Criminal Procedure Code, 1973. Sections 69A and 79 of the IT Act permit executive authorities to order the blocking of online information on similar grounds as present in Article 19(2) of the Constitution of India. Procedural guidelines have also been laid down to restrict how the state may exercise its powers of censorship.[38] The provisions of these laws provide great latitude to the government to censor online content.[39] Notably, the Blocking Rules have been used to ban thousands of websites every year, including relatively innocuous services such as Github and Sourceforge.[40]

In addition to the use of the Blocking Rules, Indian authorities frequently rely on generic provisions such as Section 144 of the Criminal Procedure Code, 1973, to restrict access to content on the Internet.[41] This power has been used more frequently in recent years for reasons ranging from the prevention of violence to the prevention of cheating in exams (Bhatia, 2017a).[42]

As mentioned previously, localisation need not *ipso facto* render content more susceptible to censorship. Censorship is a function of the domestic legal system – both in terms of the latitude it provides to state agencies acting within the scope of the law, as well as the deterrance against using extra-legal measures. What the growing number of shutdowns in India demonstrates is that the Indian state is increasingly resorting to broad based censorship measures in the digital space. Given the rising instances of online censorship in the country, it is possible that localisation may provide another tool for the state to carry out censorship more easily and effectively. In addition to the ease of being able to apply Indian laws to establishments located within the country, one may also consider, for instance, whether the government could apply Section 144, CrPC to server farms thereby prevent access to content hosted domestically. Such a restriction may render the content inaccessible anywhere in the world – not just in the relevant areas where a public order disturbance may be feared.

While it has been argued that localisation requirements may ensure that Indian

[38]Refer to the IT (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, (Blocking Rules), as well as the IT (Intermediaries Guidelines) Rules, 2011.

[39]See Pahwa (2015) and Bhatia (2015).

[40]See SFLC (2015) and SFLC (2014) on scale of banning of websites and Panday (2016) and Wikipedia (2016) for examples of some known incidents.

[41]Section 144, authorises the use of prohibitory orders to prevent public order disturbances. The provision was originally sused to secure the public from damage and prevent law and order situations from spiraling out of control (Bhatia, 2017a). However, more recently, the provision is being used to force telecom service providers to disconnect or shutdown the Internet in any given area (Hariharan & Baruah, 2015).

[42]There were 172 instances of Internet shutdowns recorded in India between January 2012 and April 2018. Of these, the highest number of 70 shutdowns were observed in 2017 (SFLC, 2018).

data continues to be available in the case of disconnection from the broader Internet, we believe this to be improbable and insufficient justification to impose broad localisation measures. At best, this may point to the need to localise certain particularly important or sensitive types of data.

To sum up, in the absence of more general legal reform, broad data localisation requirements may indeed harm the expression rights of Indian citizens due to the increased ability of the state to restrict access to content hosted locally, as well as by limiting access to content of smaller services (domestic or foreign), which may not be able or willing to bear the costs of localisation.

4 The government functions perspective

A second set of arguments posed in the context of localisation concerns the need for the state to exercise control over the online domain in exercise of the functions of the state. These arguments are made in a variety of contexts, ranging from the need to ensure protection of citizens (for instance by taking down content that is illegal), to ensure law enforcement and regulatory agencies have access to Indian data upon request, and finally, to limit the ability of multinational corporations to avoid local laws (avoiding taxes on online service providers, the unwillingness to respond to law enforcement requests, etc). In this section, we attempt to analyse these claims in greater detail.

It is an accepted principle of international law that it is the duty of a state to ensure that individuals have an effective remedy for breach of their rights. In the online context, given that "*governments no longer have the ability to easily enforce laws, manipulate data and information flows and secure privacy and security...*" (Sargsyan, 2016), it is arguable that localisation mandates may promote rights protection of domestic citizens by enhancing the enforcement capabilities of the state. For instance, in the case of data hosted abroad, an Indian citizen may not have an effective remedy against foreign based services providers (as this may require filing of claims in the foreign jurisdiction). Localisation may however make it easier for local authorities to exert jurisdiction and therefore help local citizens secure effective remedies.

On the face of it, it therefore appears that localisation would aid law enforcement and other agencies implement local laws more effectively. It would not be a stretch to argue that companies are far more likely to respond to requests from local law enforcement in circumstances where these agencies are in a position to take punitive action against physical infrastructure or personnel. However, this comes

with certain caveats.

First, with the growing usage of encryption techniques, localisation in itself may not be a sufficient tool to achieve the desired level of access. As an example, consider the Apple-FBI imbroglio in the United States, where the company refused government requests for help in decrypting data stored in a device in the government's jurisdiction (Khamooshi, 2016). Governments may therefore need to follow additional legal processes or resort to extra legal means to coerce compliance in such cases.[43]

Second, it is likely to prove difficult to enforce localisation mandates *per se*(Chander & Le, 2015). Given the technical difficulty with enforcing localisation norms, while it is likely that most law abiding actors will indeed comply, scofflaws can continue to act in violation of the law. Further, localisation norms could drive criminal elements to use more privacy enhancing technologies that may undermine enforcement capabilities further (Chander & Le, 2015). Data localisation will not imply that it will become impossible to send data packets out of the country – it would merely make this difficult and subject to legal action. A person acting in bad faith could therefore continue to transfer data abroad despite such a provision. Having said that, it must be kept in mind that a large proportion of data requests by the government are to the biggest online actors - Google, Facebook, etc. It is unlikely that such entities would actively disregard the domestic law in a jurisdiction as large and economically important to them as India.

While Indian authorities have repeatedly pointed to the need for and apparent unwillingness on the part of global intermediaries such as Google and Facebook to comply with government requests for information, as noted by the Srikrishna Committee (2018), this does not necessarily imply a recalcitrance on the part of these businesses to comply. It may, for instance, indicate vague or improper requests being made on the part of the government. That said, anecdotal evidence, as well as the existence of mechanisms such as the PRISM program revealed by Snowden, do show the extent of information sharing by large internet intermediaries with governments in their home countries as compared to countries such as India.

The concerns of Indian agencies largely emanate from two related issues: first, the issue of evasion of Indian laws, and the challenges to Indian jurisdiction by foreign multi-national corporations (MNCs) operating in India; and second, the

[43]In the Indian context, one may reference the Blackberry imbroglio in around 2008-13 when the government requested access to encrypted Blackberry communications. After initially refusing the government's request, Research-in-Motion eventually gave in to pressure, setting up a server in Mumbai to enable lawful access to Indian law enforcement agencies (Horwitz, 2013), (Bohn, 2012) and (Singh, 2012)

challenges being faced in the use of MLATs and letters rogatory (that are issued by courts), the existing mechanisms available to authorities in India for accessing evidence housed in other jurisdictions.

With respect to the first issue, government agencies have often expressed their dismay in securing compliance with domestic legal requirements by Internet-based services. For instance, in a case relating to the purported online game 'Blue Whale Challenge' the Madras High Court referred to the problems faced in conducting cyber investigations in India – many online services do not have nodal officers in India or often take the stand that the service is "*provided by another company incorporated in USA or any other foreign country and that therefore they are not in a position to furnish the information sought for*" (The Registrar (Judicial) vs Secretary, 2017).[44]

On the second issue, it has been noted that authorities are often unable to access data (or do so in a timely manner) due to complexity of the MLAT procedures and the need to satisfy the legal requirements of the other country in order to gain access to the data. For instance, the Stored Communications Act in the United States requires a warrant issued in the US before providing access to a user's content data, a process that also needs to be followed by investigating officers in India before getting access to such data from the United States (Mohanty & Srikumar, August, 2017). Further, it is also worth noting that the scope of MLATs and similar arrangements is limited to exchanging or procuring data that is required for the purposes of criminal proceedings. Information pertaining to general compliance requests from regulatory bodies would therefore not fall within the ambit of such frameworks.

The Telecom Regulatory Authority of India (TRAI) has, in its Recommendations on Cloud Services (August 2017), suggested dealing with these issues by: (a) signing more comprehensive MLATs with a wider range of countries (India currently has signed MLATs with only 39 countries); (b) ensuring MLATs are sufficiently detailed to resolve differences in interpretation of laws; and (c) ensuring the inclusion of provisions that enable speedy processing of requests (including through the use of electronic systems). The Indian government could also, at least in the context of US based companies, use the CLOUD Act[45] to secure easier access to Indian data held by them.

[44]Other prominent cases involving regulation of online intermediaries and services have arisen in the context of the Facebook-Whats App privacy policies, online pornography, advertisements on pre-natal sex determination tests and videos of sexual violence. See (Chawla, 2017).

[45]The legislation empowers executive agencies in the US and India to enter into an agreement whereby Indian executive agencies would be able to directly secure access to information pertaining to non-US persons from US based companies.

It therefore appears that to the extent that government access is the issue, there may be certain less intrusive measures that could be explored in order to achieve the same ends. A precondition to this would be the need to identify the specific problem being faced by law enforcement or other regulatory agencies in accessing any particular type of data (which may be held by communication providers, intermediaries or regulated agencies). This will enable more targeted interventions to be considered rather than implementing sweeping localisation norms. Such measures may include limited localisation, say by requiring a copy to be retained within the country, where it can be demonstrated that immediate and on-demand access to specific types of data is necessary for the discharge of certain functions.

Another argument that has been raised by some domestic firms while making a case for localisation by competing foreign firms is that the absence of localisation allows "*foreign companies to exploit local market data without paying fair taxes*" (PhonePe, 2018). This is supported by the view that hosting of local servers in the territory of a country would make it possible to assert the existance of a 'fixed place of business', hence attracting taxation provisions by virtue of becoming a permanent establishment (Collin & Colin, 2013). The need for data localisation to achieve this end has however come into question in light of new thinking on the exercise of taxation powers in the digital economy. Borrowing from the option suggested under Action Plan 1 of the Organisation for Economic Co-operation and Development's work on Base Erosion and Profit Shifting, the Finance Act, 2018 introduced an amendment to the income tax law in India to incorporate the concept of 'significant economic presence'.[46]

As per Section 9, Explanation 2A of the Income Tax Act, 1961, significant economic presence[47] of a non-resident in India would constitute a 'business connection', hence making such income taxable in India. The provision also clarifies that whether the non-resident has a residence or place of business in India would not be relevant for determining the existence of a significant presence. Besides this, India has already adopted an 'equilisation levy' since 2016 that provides for the imposition of taxes on advertising revenues earned by foreign firms through business carried out in India without having a permanent establishment here (Jha,

[46]See OECD (n.d.) and Patnaik (2018). The OECD previously maintained that there was a distinction between the physical location of servers, which involve a physical presence, as opposed to 'data' and 'software' that cannot constitute a permanent establishment since they do not involve any tangible property (Collin & Colin, 2013).

[47]Defined to mean (i) a transaction in respect of any goods, services or property carried out by a non-resident in India, including provision of download of data or software in India, if payments arising from such transaction exceed a prescribed amount; or (ii) systematic and continuous soliciting of business activities or interaction with more than a prescribed number of users through digital means.

2018). The initiation of these moves weakens the argument of using taxation as a justification for data localisation.

5 The economic perspective

The growth of the Internet and accompanying data flows have been key drivers of economic growth in the last few decades. Localisation demands, however, seem to ignore the fact that one of the benefits of the Internet has been to create efficiencies through enabling the global distribution of data and services. A study by Mckinsey Global Institute found that in 2014 the direct impact of cross-border data flows had raised world GDP by 3 percent (worth about $2.2 trillion in 2014), which exceeded the contribution of trade in traditional goods in that year (Manyika et al., 2016).[48]

Yet, the oft-cited references to data being "the new oil" also come with the realisation that a handful of corporations (the likes of Google, Amazon, Apple, Facebook and Microsoft) exercise significant control over this resource (The Economist, 2017). In terms of hosting locations, 42 percent of the world's top million sites are based in the United States and Canada, 31 percent in Europe, only 12 percent in the Asia Pacific region and the remaining in other parts of the world (Manyika et al., 2016). The measures being adopted to bridge these gaps range from a push for tighter regulation of the technology sector to looking at data localisation as a tool to promote the domestic industry. India's recent policy push towards localisation also refers to goals like "nurturing digital innovation" and "stimulating domestic digital economy" (e-Commerce Task Force, 2018). Similarly, the Srikrishna Committee's report refers to the *"positive impact of server localisation on creation of digital infrastructure and digital industry"*.

In examining the effect of localisation measures on the economy, one must also relate this with the impact that it would have on individual businesses. Article 19(1)(g) of the Constitution protects the freedom to practice any profession, or to carry on any occupation, trade or business. As with other fundamental rights, this right is also subject to certain reasonable restrictions. Restrictions in this regard may be imposed on grounds of the activity being anti-social or against public welfare, in addition to the specific grounds in Article 19(6).[49] Notably, the government

[48] Adding to this the *indirect* impact in terms of the impact of cross-border data transfer in enabling other types of flows (like transfer of goods through global e-commerce), Manyika et al. (2016) found that the contribution would be closer to $2.8 trillion.

[49] Sodan Singh v. New Delhi Municipal Corporation, 1988. The scope of the right to business in india, however, does not extend as far as under the European Charter of Fundamental Rights

may impose licensing and other conditions on businesses.[50] Accordingly, the state may legitimately impose restrictions on cross-border flows of data in the interests of public welfare, despite the apparent costs that it may impose on businesses.

While it may be difficult to demonstrate that localisation measures would result in the violation of a the rights under Article 19(1)(g), the effects of localisation on businesses should nevertheless be a consideration from a policy perspective. The increasingly intertwined nature of the economy with the Internet implies that curbs on online businesses would necessarily have several economic implications. In this section we unpack the arguments around measuring the economic impact of data localisation, on domestic industries as well as global businesses. This is followed by a discussion on the broader debates around localisation in the context of international trade agreements.

5.1 Measuring the economic impact

One of the main arguments against mandatory localisation stems from the cost that it is likely to impose on businesses and consequently, their consumers and the economy as a whole. Widespread localisation norms will mean that businesses and other users – both domestic and foreign – will no longer have the flexibility to choose the most cost-effective or task-specific location to store their data. These efficiency losses will ultimately be passed onto consumers in the form of higher costs of service. While the literature on data localisation frequently makes these assertion, only a handful of studies have attempted to undertake an actual cost-benefit analysis of data localisation measures.[51]

5.1.1 Costs of data localisation

Despite the lack of significant economic literature on this subject, the purported costs of localisation measures are often raised as a ground to argue against the imposition of such measures. Most commentators refer to just two prominent studies on this subject – a 2014 study by the European Centre for International Political Economy and another one in 2015 by Leviathan Research (in association with Google) – both of which note that the costs of localisation outweight its

and Freedoms (EUChFr), which has been interpreted more broadly, to include the economic interests connected with running a business (Carss-Frisk, 2001).

[50]For instance, licensing for cable TV operators was held to be legal and not a restraint on trade in Shiv Cable v. State of Rajasthan (1993).

[51]Bauer, Lee-Makiyama, der Marel, and Verschelde (2014), Bauer, Ferracane, and van der Marel (2016) and Leviathan (2015).

benefits. While the findings of these studies remain contested (Gurumurthy & Chami, 2017), in the absence of any other evidence on this subject, we find it useful to examine the findings of these reports in some detail.

In the study conducted for the European Centre for International Political Economy, Bauer et al. (2014) quantify the expected losses from data localisation requirements and related measures in seven jurisdictions, including India.[52] They find that imposing economy-wide data localisation requirements could reduce the Indian GDP by 0.8 percent and domestic investments by 1.4 percent.[53] The study also looked ay the welfare costs of data regulation on a per worker basis and find that for India, the loss per worker would be equivalent to 11 percent of the average month salary. The authors finally conclude that *"any gains stemming from data localisation are too small to outweigh losses in terms of welfare and output in the general economy".*

Building further on this study, Bauer et al. (2016) found that the impact of data localisation on specific sectors varies depending on the extent to which a particular sector is dependent on data inputs. As a result, the negative impact was found to be higher for sectors like communication services, financial services and other data-intensive businesses. This led the authors to conclude that tighter restrictions of free flow of data would cause an economy's production structure to shift back towards sectors such as agriculture, raw materials and natural resources.

Moving away from the macro-level approach of the above studies, Leviathan (2015) looked at the effect of forced data localisation laws on individual businesses by calculating the cost difference on a per-hour, per-server level. The study focused on public "Infrastructure as a Service" (IaaS) cloud computing providers and found only seven cloud providers globally met the selected criteria.[54] None of the identified providers had data centers in India. As a result, domestic users would either have to use traditional datacenters, with accompanying capital investment in hardware and periodic upgrade costs, or they would have to enter into specifically negotiated business contracts with non-public cloud providers. In case of countries that did have such data centers, the reserchers found that forced data localisation laws would require local companies to pay 30-60 percent more for their

[52]Besides localisation requirements, the study also takes into account other legal obligations that may increase compliance costs, such as consent requirements, right to review personal information, security breach notifications, etc.

[53]Imposing even sectoral data protection norms could arguably have a similar (albeit smaller) effect on the economy, particularly in the short to medium term as online businesses and service providers work to recalibrate their supply chains and infrastructure in India.

[54]Amazon Web Services, DigitalOcean, Google Compute Engine, HP Helion Public Cloud, Linode, Microsoft Azure and Rackspace Cloud Servers. It is worth noting however that the funding for this study was provided by Google.

computing needs if the data had to be housed in a local server.

5.1.2 Impact on the domestic industry

Information technology (IT) is one of the key sectors in India's growth story, which contributed about 7.9 percent of India's GDP in the year 2017-18 (MeITY, 2018). The export of IT services and the outsourcing industry, also referred to as business process management (BPM), contributed about 51 percent and 21 percent, respectively to India's IT exports in the previous year.[55] India's advantage in the sourcing sector is also evident from the fact that it accounted for approximately 55 percent market share of the $ 185-190 billion global services sourcing business in 2017-18 (IBEF, 2018).

This makes it important for the policy framework in India to consider the strategic impact of its localisation moves on the domestic IT services industry.[56] On one hand, there is a recognition that the "*development of automation technology and increasingly protectionist measures globally*" are resulting in changing global demands, which will have significant implications for the Indian outsourcing industry (NITI Aayog, 2018). On the other, it remains true that despite these shifts, the sector will continue to remain relevant for India in the short to medium term. Therefore, India's role in furthering a global push towards increased data localisation needs to be considered more carefully, since the implementation of any reciprocal localisation measures may dramatically affect the development of this sector. This is also vital from a long term economic perspective. Given India's dominant position in the business processing and outsourcing industries, implementing measures that could hamper growth of this sector would appear detrimental to its national economic interests. One should also keep in mind that as global businesses grow, they also seek to leverage domestic skill sets to service global clientelle. For instance, Cisco has established global development centres in India to take advantage of the the large number of engineering students in the country.[57] Similarly, Google houses many of its research centres in locations around the world, including India. Broad localisation measures may impact the

[55] In the financial year 2017-18 the Indian IT industry was worth $167 billion of which $126 billion was in exports (IBEF, 2018).

[56] When the IT rules were notified for the protection of sensitive personal data there was some uncertainty around their application to the outsourcing industry. This led to a clarification from the government that the requirement to obtain consent from users was not applicable to outsourcing service providers servicing other companies based in India or abroad (Hunton, 2014).

[57] Cisco's Bangalore centre, the largest facility outside the US, has apparently filed for over 1000 of the company's patents (Manyika et al., 2016).

way such globalised businesses function, thereby affecting India's developing software industry and by implication its economic interests.

That said, one of the arguments used in favour of data localisation is that it would provide a boost to the local computer hardware and software industry and generate local employment. Researchers have contested this view on the following grounds. First, bulk of the capital goods (diesel generators, cooling systems, servers, and power supply devices) that are deployed in the creation of data centers are generally imported from global suppliers (Chander & Le, 2015). Second, while the building of data centers will involve the engagement of construction workers in the initial phase, the actual running of the centers does not generate much direct employment. Cory (2017) illustrates this with the example of a $1 billion data center built by Apple in North Carolina, United States in 2011, which created only 50 full-time jobs and another 250 support jobs in areas such as security and maintenance.

Another powerful narrative that has emerged in recent times is about the need for domestic mechanisms for the creation, sharing and use of data for the development of artificial intelligence (AI) development. To quote from the Srikrishna Committee's report, *"The growth of AI is heavily dependent on harnessing data, which underscores the relevance of policies that would ensure the processing of data within the country using local infrastructure built for that purpose."* The Committee then goes on to note that these benefits can be achieved by ensuring that at least one copy of personal data is stored in India and that more sensitive, critical personal data is processed and stored only in India. The flaw of this argument lies in the assumption that mere storing data of data in India would automatically make it accessible for all sorts of beneficial research. Assuming all the big MNC companies do agree to localise data produced by Indians, this data would still continue to be held by foreign MNCs. Physically locating the data in India would not really enhance the ability of Indian companies to access it.

Given that the data in question is personal and sensitive and critical personal data of individuals, its use will be governed by the protections under the proposed data protection law. Within the scope of the legal framework, the authority to decide on the purposes for which the data will be used vests with the 'data principal' or the 'data fiduciary' – defined in the draft Bill to mean the person who alone or in conjunction with others determines the purpose and means of processing of personal data.[58] Therefore, unless the state proposes to use other tools for the coercion of data disclosure by private entities, its storage or processing in India would not lead to any automatic benefits for AI development. Of course, this may not be the case should foreign companies refuse to localise and exit the Indian market.

[58]Section 3(13), Protection of Personal Data Bill, 2018.

In any event, to the extent that the draft Bill allows for the exclusion of anonymised data and exceptions for use of personal data for research purposes, these provisions would be applicable irrespective of the where the data is stored. Therefore anonymised data - irrespective of where it is held - can be put into the public domain in India for the benefit of any interested parties. Localisation measures (or the absence of such measures) would have no bearing on this.

5.1.3 The global nature of modern businesses

With the growth in global trade and services, many businesses require the flexibility to analyse large volumes of data from across different jurisdictions. For instance, in the context of online payments, real time fraud detection relies on noting unusual payment patterns across jurisdictions. Equally, issues such as transnational crime, money laundering, etc., involve processing data from multiple jurisdictions (Srikumar & Mohanty, 2018). Businesses also derive efficiency gains from being able to leverage the economies of scale derived from having common processes for all their data. A data localisation requirement would therefore have significant implications for how existing systems are designed and implemented. Specifically in the context of the draft Personal Data Protection Bill, 2018, which only requires localisation of personal data covered by the law (i.e. Indian personal data), businesses will have to segregate their user data based on the location of the user, and the type of data. This would be in addition to the costs of procuring additional infrastructure within the country.

Chander and Le (2015) note that localisation requirements also interfere with the access to technologies like cloud computing, the Internet of Things, and big data analytics. The authors elaborate that localisation threatens big data in at least two ways – by imposing limits on data aggregation due to increased costs and complexity; and eroding the informational value that can be gained from cross-jurisdictional studies. Further, localisation may also deter businesses from, or reduce the effectiveness of, practices such as 'sharding'[59] of databases, which improves performance and helps in protection of the data.

While it is difficult to assess the extent to which localisation requirements may deter the entry of new players or impede the growth of existing businesses, some trends can be expected. First, despite posing the strongest resistance, large global players will be better positioned to absorb the additional costs of localisation compared to smaller players. This will serve to strengthen their dominance in various

[59]Sharding involves dividing databases into discrete parts, allowing for smaller more easily managed portions of large databases to be kept at different locations.

sectors, at least in the short run.[60] Second, localisation will create entry barriers for certain types of service providers for whom India is not significant enough a market to justify the costs of localisation.[61] This, as discussed previously, can potentially impact the ability of consumers to access new and innovative services.

5.2 Readiness of India's data center infrastructure

While discussing the costs and benefits of localisation it is also relevant to keep in mind the reality of India's current data center capabilities. In the absence of external pressures, an entity's decision about the location of data centers is based on a number of factors, which may be *geographic* – firms may choose to locate close to core customers or seek cooler climates; *economic* – the costs of electricity, infrastructure facilities, tax structures; *technical* – link with core backbone networks or *political* – low political risks (Azmeh & Foster, 2016). It therefore becomes relevant to question how India fares on these parameters in terms of being a viable location for the setting of data centers and creation of cloud storage facilities.

A Gartner study in 2015 found that India held just about 1.2 percent of the world's data center infrastructure and 5.23 percent in the Asia-Pacific region (IAMAI, 2016). Taking into account factors like energy cost, international bandwidth, ease of doing business and taxation provisions, Cushman & Wakefield (2016) Data Center Risk Index score placed India at thirty sixth position, with a score of 47.84 (out of a highest score of 100).[62] In terms of the readiness of India's cloud ecosystem, ACCA (2018) scored India at 49.1 out of 100 (twelfth out of fourteen Asian countries in the study) on its 'Cloud Readiness Index'. To provide some context, India fares worse than other developing countries like Brazil, South Africa, Indonesia and Malaysia, although it does better than China and Vietnam. A large part of this attributed to the weakness of our cloud infrastructure.

Moreover, studies have also show that India is a relatively expensive destination when it comes to the issue of affordability of cloud hosting services. The Cloud Security Alliance's 2017 Report on the State of Cloud Adoption in Asia Pacific ranks

[60] Early data on implementation of the GDPR indicates that large companies are far better positioned to meet compliance requirements of strict data protection laws (Kostov & Schechner, 2018).

[61] The experience in EU shows that the mere imposition of higher data protection standards (without mandating localisation) also affects service provision. This can be seen from examples of various online gaming sites that decided to withdraw access to European users post the implementation of the GDPR in May, 2018 (Andres, 2018).

[62] The top three destinations as per this index are Iceland, Norway and Switzerland, which score in the range of 90 to 100.

India at number 10 out of 11 countries studied for affordability of cloud services after adjusting for cost of living (Choi, Huang, & Law, 2016). This is taking into account factors like the cloud service cost, Internet cost, basic utilities cost and rental cost. Therefore, the data center infrastructure in India continues to be underdeveloped due to the costs involved in building large data centres, the absence of proper downstream infrastructure such as uninterrupted power supply as well as weather conditions in India which necessitate greater expenditure on cooling.[63] Essentially, present conditions make it uneconomical and inefficient to host large quantities of data in India (Ajay Shah, 2015). The e-Commerce Task Force (2018), also acknowledges this fact and hence highlights the need for capacity development in terms of infrastructure for data centres, improvements in power supply and tax benefits before mandating full data localisation. Similar recommendations were also made by the Internet and Mobile Association of India, which highlighted the various legal, policy and regulatory enablers needed to promote the data center industry in India. The report also cautioned against mandatory data localisation norms, *"which would reduce competitiveness and would have a deterring impact on the GDP of the economy and drive away India's extensive ability to attract data centre investments"* (IAMAI, 2016).

5.3 Localisation debates in trade agreements

The growing importance of global e-commerce has placed data localisation debates at the heart of many international trade discussions. The United States has been at the forefront of pushing for the removal of various kinds of restraints on cross-border trade carried out through electronic means. This includes demands for "enabling cross border data flows" and "preventing localisation barriers" (United States, 2016).[64] Despite these attempts by a number of countries including the United States, Canada and Japan, the current e-commerce discussions at the World Trade Organization (WTO) level are limited to discussions without any rule-making mandate (Macleod, 2015).[65] A broadening on this mandate has however been resisted by many developing countries, including India. Several groups

[63]These costs may however come down in the future with the adoption of experimental technology like Microsoft's Natick data centre that involves placing the data centre just off the coast, hence drastically reducing the cooling costs (Roach, 2018).

[64]The United States is also following a similar strategy in bilateral discussions. Two US Senators recently wrote to India urging it to adopt a 'light touch' regulatory framework that would allow data to flow freely across borders (Kalra, 2018).

[65]The Declaration on Global Electronic Commerce adopted by the WTO General Council in 1998 established a Work Programme on Electronic Commerce. The Work Programme is mandated "to examine all trade-related issues relating to global electronic commerce, taking into account the economic, financial, and development needs of developing countries".

oppose this sort of a 'mission creep' at the WTO on the ground that it would lead to developing countries being required to sign away their right to strategically regulate the digital market and data flows (Gurumurthy & Chami, 2017).[66]

Data localisation norms also stand to be challenged under the existing provisions of the WTO's General Agreement on Trade in Services, 1995 (GATS).[67] In September, 2017, the United States initiated a communication before the Members of the Council for Trade in Services questioning China's new Cyber Security Law. Through this law, China has mandated that all 'personal information' and 'important data' collected or generated by critical information infrastructure operators must be stored in the country. The law came into effect in June, 2017 but the localisation provisions are expected to come into force only by the end of 2018 (Chin, Goodell, Liu, & Zhang, 2018).[68] The communication from the Unites States claims that these measures would *"disrupt, deter, and in many cases, prohibit cross-border transfers"* of many *"expansive and loosely-defined categories of data"* (United States, 2017).[69]

While the global e-commerce discussions under the WTO have not managed to progress, provisions relating to cross-border trade and localisation of data have found their way into other multilateral arrangements. Prominent among these are the recently signed Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the ongoing discussions on the Regional Comprehensive Economic Partnership (RCEP). The CPTPP incorporates by reference the provisions of the Trans-Pacific Partnership Agreement (TPP), Chapter 14 of which included provisions on e-commerce. It contains commitments for cross-border transfer of information (including personal information) and a restriction on measures mandating local hosting of computing facilities, subject to legitimate public policy objectives that are non-arbitrary, proportionate and do not amount to a disguised restriction on trade. Similar, though somewhat more stringent provisions are found in the US-Mexico-Canada (USMCA) free trade agreement (which replaces the North American Free Trade Agreement (NAFTA))[70]; and some ob-

[66] As an aside, it is interesting that countries such as the US - which have vociferously championed a multistakeholder model for Internet related governance, seem to be more than willing to take this issue to a multilateral forum such as the World Trade Organisation (WTO) arrangement.

[67] See Greenleaf (2016) and Greenleaf (2018).

[68] While the law provides that the data localisation requirement applies only to critical information infrastructure, subsequent draft implementation rules and guidance indicate a broader remit that will also include other network operators (Chin et al., 2018).

[69] It is also reported that the US may consider raising objections to the localisation measures in the draft Personal Data Protection Bill, 2018, during upcoming India-US trade talks in September 2018 (Kalra & Shah, 2018).

[70] Article 19.11 of the USMCA bars restrictions on cross-border transfer of information, subject

servers believe that the US will attempt to impose such provisions in other trade agreements also.

In case of the RCEP negotiations, in the absence of a draft of the negotiating text we do not know the exact nature of the provisions that will be in its e-commerce chapter, although it has been suggested that this may be *"less ambitious and contentious than that of the TPP"* (Panday, 2017). Given, the recent policy trends in India and the country's resistance to e-commerce negotiations at the WTO level, it seems likely that India will not support the introduction of restrictions on cross-border data transfers and anti-localisation norms in RCEP and other multilateral trade agreements.

The position adopted by those who seek to include data flow related issues in trade agreements appears to be based on the notion that personal data must be treated as any other commodity. Accordingly, free flows of data must be the de facto position unless justified by overwhelming public policy concerns. What constitutes a legitimate public policy concern would be adjudicated at the international level, under the WTO framework.[71] However, this approach has been challenged on three grounds – first is the the rights-based argument that sees personal data as essential to a person's autonomy and identity and therefore as more than a mere commodity; second, is the fact that commercial exploitation and trade in commodities of various kinds are indeed regulated or taxed; and third, that the use of WTO mechanisms reduces democratic control over data (R. Hill, 2017). As explained previously, the free flow of data is seen to strengthen the position of global incumbents in the digital economy – large, monopolistic Internet corporations don't pay sufficient taxes or other dues across the world, in addition to which they make huge profits without adequately compensating the individual's whose data these profits are built upon. Accordingly, there is a percieved need to to recalibrate the nature of the digital economy, through taxation, localisation measures, and the like.

To conclude, irrespective of whether one consideres trade negotiations to be an appropriate location to discuss trans-border data flows, one would venture that untill such time as there is broader recognition of the rights based, economic and strategic concerns of developing nations, who see mostly US based mega-corporations cornering large chunks of the digital economy pie, any broader resolution of the issue appears unlikely.

to similar restrictions as in the TPP/CPTPP. Article 19.12 of the USMCA prohibits the imposition of measures mandating the use of local computing facilities as a precondition for conducting business within the territory of a country. Unlike the TPP/CPTPP, there are no derogations permitted from this provision.

[71] See R. Hill (2017).

6 Conclusion

We examined the three main sets of arguments that are generally used for making a case for data localisation. First, there is the claim that local hosting of data will enhance its privacy and security by ensuring that an adequate level of protection is given to the data. Second, it is argued that lack of government access to data (due to it being stored in another jurisdiction) impedes the law enforcement and regulatory functions of the state, which can be addressed through localisation. Third, there is the narrative on the economic benefits that will accrue to the domestic industry in terms of creating local data infrastructure, employment, and contributions to the AI ecosystem.

Following an assessment of each of these perspectives we find that the costs of introducing broad and sweeping data localisation norms are likely to outweigh its benefits, from a rights-based perspective as well as an economic one. Yet, this is not to suggest that data localisation can never quality as a justified measure. There may indeed by circumstances where local storage (and even processing) of the data can be justified, particularly on certain normative grounds. In order to identify such instances and arrive at a narrowly tailored response, we propose that the policymaking process should include the following steps.

- Identification of the specific problem that is sought to be addressed, along with the evidence indicating the scale of the problem.
- Evaluation of the various options being considered to address the issue, along with the expected costs and benefits of each alternative. The goal here would be to identify if data localisation can stand the test of being the least intrusive mechanism to address the problem at hand, as well as the proximity of the measure to the harm sought to be prevented against. This analysis should take into account a broad range of factors, including the impact of the proposed measures on civil liberties, functioning of the state and economic implications for all stakeholders.
- Among the range of localisation options that are available, the preference should be to begin by considering the least intrusive measure (conditional transfers of data) before moving towards the most onerous requirement of storage and processing only within the territory.
- This entire process should be carried out in an open and transparent manner providing the affected parties and the public at large the opportunity to question and strengthen the analysis.

Specifically, in the context of the draft data protection bill proposed by the Srikrishna

Committee, the above process can be built into the proposed law instead of the existing proposal of having a data mirroring requirement for all personal data and additional local processing requirements for some other categories.

It would be advisable to defer any general policy directives on localisation, whether for categories of personal data or otherwise, until a more robust study of the issues has been conducted. At the same time, India must also resist the pressure to enter into bilateral or multilateral trade agreements that constrain its ability to take future decisions on data localisation in particular, or more generally, its broader stance on e-commerce. India's position on data localisation must ultimately be weighed against the government's aspirations to create a 'Digital India' and the need for strategic thinking on whether a closed data economy or an open one would be more conducive to meeting those goals.

References

ACCA. (2018). *Cloud readiness index*. Asia Cloud Computing Association. Retrieved from http://www.asiacloudcomputing.org/research/2018-research/cri2018

Ahmed, U. & Chander, A. (2016, February). Information goes global: protecting privacy, security, and the new economy in a world of cross-border data flows. UC Davis Legal Studies Research Paper Series Research Paper No. 480. Retrieved from http://ssrn.com/abstract=2731888

Andres. (2018). The balkanisation of the internet. Technolama. Retrieved from https://www.technollama.co.uk/the-balkanization-of-the-internet

Azmeh, S. & Foster, C. (2016). The tpp and the digital trade agenda: digital industrial policy and silicon valley's influence on new trade agreements. London School of Economics Working Paper Series. Retrieved from http://www.lse.ac.uk/international-development/Assets/Documents/PDFs/Working-Papers/WP175.pdf

Bailey, R., Bhandari, V., Parsheera, S., & Rahman, F. (2018, August). Use of personal data by intelligence and law enforcement agencies'. National Institute of Public Finance and Policy. Retrieved from http://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf

Basu, D. D. (2012). *Commentary on the constitution of india*. 8th edition, Volume 2, LexisNexis Butterworths Wadhwa.

Bauer, M., Ferracane, M. F., & van der Marel, E. (2016). *Tracing the economic impact of regulations on the free flow of data and data localization*. Centre for International Governance Innovation and Chatham House. Retrieved from https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf

Bauer, M., Lee-Makiyama, H., der Marel, E. V., & Verschelde, B. (2014). *The costs of data localisation: friendly fire on economic recovery*. European Centre for International Political Economy. Retrieved from http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf

Bhan, S. (2018). Exclusive: govt decides to drop draft e-commerce policy. Twitter, 17 September, 2018. Retrieved from https://twitter.com/ShereenBhan/status/1041694515025850368

Bhandari, V., Kak, A., Parsheera, S., & Rahman, F. (2017, 20 September). An analysis of puttaswamy: the supreme court's privacy verdict. The Leap Blog. Retrieved from https://blog.theleapjournal.org/2017/09/an-analysis-of-puttaswamy-supreme.html

Bhargava, Y. (2016, August). Trai rules in favour of net neutrality. The Hindu. Retrieved from https://www.thehindu.com/sci-tech/technology/internet/TRAI-rules-in-favour-of-Net-neutrality/article14068029.ece

Bhatia, G. (2015, 25 March). The supreme court's it act judgment, and secret blocking. Indian Constitutional Law and Philosophy Blog. Retrieved from https://indconlawphil.wordpress.com/2015/03/25/the-supreme-courts-it-act-judgment-and-secret-blocking/

Bhatia, G. (2016, November). Violent words, free speech and the indian constitution. Live Mint. Retrieved from https://www.livemint.com/Sundayapp/UE9YldojhVlWnSI877F4FJ/Violent-words-free-speech-and-the-Indian-Constitution.html

Bhatia, G. (2017a, October). Making the internet disappear. The Hindu. Retrieved from https://www.thehindu.com/opinion/lead/making-the-internet-disappear/article19877770.ece

Bhatia, G. (2017b, August). The architecture of censorship. The Hindu. Retrieved from https://www.thehindu.com/todays-paper/tp-opinion/the-architecture-of-censorship/article19505826.ece

Bohn, D. (2012, February). Rim sets up blackberry server in mumbai, continues to offer 'lawful access' to indian government. The Verge, 22 February 2012. Retrieved from https://www.theverge.com/2012/2/22/2818195/rim-sets-up-blackberry-server-in-mumbai-continues-to-offer-lawful

Borger, J. (2013, February). Nsa files: what's a little spying between friends. The Guardian. Retrieved from https://www.theguardian.com/world/2013/dec/02/nsa-files-spying-allies-enemies-five-eyes-g8

Canatacci, J. (2018, 28 February). Report of the special rapporteur on the right to privacy, advance unedited version. A/HRC/37/62. Retrieved from https://www.ohchr.org/en/hrbodies/hrc/regularsessions/session37/documents/a_hrc_37_62_en.docx

Carss-Frisk, M. (2001, November). The right to property: a guide to the implementation of article 1 of protocol no. 1 to the european convention on human rights. Human Rights Handbook No. 4, Council of Europe. Retrieved from https://rm.coe.int/168007ff4a

Chander, A. (2011, 28 February). Googling freedom. California Law Review, Vol. 99, Issue 1. Retrieved from https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1049&context=californialawreview

Chander, A. & Le, U. P. (2015). Data nationalism. *Emory Law Journal*, *64*(3). Retrieved from https://ssrn.com/abstract=2577947

Chawla, A. S. (2017, December). The supreme court's free speech to-do list. The CCG Blog. Retrieved from https://ccgnludelhi.wordpress.com/tag/kamlesh-vaswani/

Chin, M., Goodell, A., Liu, C., & Zhang, X. (2018). China's cybersecurity law. Reed Smith. Retrieved from https://www.reedsmith.com/-/media/files/perspectives/2018/chinas-cybersecurity-law-002.pdf

Choi, V., Huang, S., & Law, M. (2016). *State of cloud adoption in asia pacific*. Cushman & Wakefield. Retrieved from https://downloads.cloudsecurityalliance.org/assets/%20survey/State%20of%20Cloud%20Adoption%20in%20APAC%202017.pdf

Cohen, B., Hall, B., & Wood, C. (2017). Data localisation laws and their impact on privacy, data security and the global economy. Antitrust, Vol. 32, No. 1, Fall. Retrieved from https://www.americanbar.org/content/dam/aba/publications/antitrust_magazine/anti_fall2017_cohen.authcheckdam.pdf

Collin, P. & Colin, N. (2013, January). *Task force on taxation of the digital economy*. Report to the Minister for the Economy, Finance, and others, Government of France. Retrieved from https://www.hldataprotection.com/files/2013/06/Taxation_Digital_Economy.pdf

Connolly, K. (2018, 25 May). Gdpr: us news sites unavailable to eu users under new rules. BBC. Retrieved from https://www.bbc.com/news/world-europe-44248448

Cory, N. (2017, May). *Cross border data flows: where are the barriers and what do they cost?* Information Technology and Innovation Foundation. Retrieved from https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost

Cushman & Wakefield. (2016). *Data center risk index*. Cushman & Wakefield. Retrieved from http://www.cushmanwakefield.com/en/research-and-insight/2016/data-centre-risk-index-2016

DeITY. (2015, December). *Request for proposal for provisional empanelment of cloud service providers*. Department of Electronics and Information Technology. Retrieved from http://meity.gov.in/writereaddata/files/RFP_CSPs_10_16.pdf

EC Staff Document. (2017). *Commission staff working document on the free flow of data and emerging issues of the european data economy*. European Commission. Retrieved from https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy

e-Commerce Task Force. (2018). Electronic commerce in india: draft national policy framework (non-official version). Medianama. Retrieved from https://www.medianama.com/wp-content/uploads/Draft-National-E-commerce-Policy.pdf

European Data Protection Supervisor. (2014, 23 June). Opinion on the commission communication on internet policy and governance - europe's role in shaping the future of internet governance. European Data Protection Supervisor. Retrieved from https://edps.europa.eu/sites/edp/files/publication/14-06-23_internet_governance_en.pdf

Ferracane, M. F. (2017, November). *Restrictions on cross-border data flows: a taxonomy*. European Centre for International Political Economy. Retrieved from http://ecipe.org/publications/restrictions-to-cross-border-data-flows-a-taxonomy/?chapter=3

Ferracane, M. F., Lee-Makiyama, H., & der Marel, E. V. (2018). *Digital trade restrictiveness index*. European Centre for International Political Economy. Retrieved from http://ecipe.org/app/uploads/2018/04/DTRI-final1.pdf

FSDC. (2013, 24 October). Eigth meeting of the financial stability and development council. Department of Economic Affairs, Ministry of Finance.

Gallagher, R. & Greenwald, G. (2014, December). How the nsa plans to infect 'millions' of computers with malware. The Intercept. Retrieved from https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/

Geist, A., Gjerding, S., Moltke, H., & Poitras, L. (2014, September). Nsa 'third party' partners tap the internet backbone in global surveillance program. Information. Retrieved from https://www.information.dk/udland/2014/06/nsa-third-party-partners-tap-the-internet-backbone-in-global-surveillance-program

George, V. K. (2018, 30 August). India, us sign military logistics pact. The Hindu. Retrieved from https://www.thehindu.com/news/international/India-US-sign-military-logistics-pact/article14598282.ece

Goldsmith, J. & Wu, T. (2006). *Who controls the internet: illusions of a borderless world*. Oxford University Press.

Greenberg, A. (2018). The untold story of notpetya, the most devastating cyberattack in history. Wired, 22 August, 2018. Retrieved from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Greenleaf, G. (2016). Free trade agreements and data privacy: future perils of faustian bargains. UNSW Law Research Paper No. 2016-08. Retrieved from https://ssrn.com/abstract=2732386

Greenleaf, G. (2018). Looming free trade agreements pose threats to privacy. *Privacy Laws & Business International Report*, *152*, 23–27.

Greenwald, G. (2014, December). How the nsa tampers with us-made internet routers. the Guardian. Retrieved from https://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden

Gurumurthy, A. & Chami, A. V. N. (2017). The grand myth of cross-border data flows in trade deals. IT for Change. Retrieved from http://itforchange.net/grand-myth-of-cross-border-data-flows-trade-deals#footnote34_7w9cffs

Hariharan, G. & Baruah, P. (2015, August). The legal validity of internet bans - part ii. The Centre for Internet and Society. Retrieved from https://cis-

india.org/internet-governance/blog/the-legal-validity-of-internet-bans-part-ii

Hetavkar, N. (2018, December). Rbi firm on data localisation; 80% of firms to comply by oct 15 deadline. Business Standard. Retrieved from https://www.business-standard.com/article/economy-policy/rbi-firm-on-data-localisation-80-of-firms-to-comply-by-oct-15-deadline-118101101302_1.html

Hill, J. (2014, July). The growth of data localization post-snowden: analysis and recommendations for u.s. policymakers and industry leaders. The Lawfare Institute, Lawfare Research Paper Series, Vol.2, No.3. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2430275

Hill, R. (2017). Second contribution to the june-september 2017 open consultation of the itu cwg-internet, why should data flow freely? Association for Proper Internet Governance, 19 June 2017. Retrieved from https://bit.ly/2QBOydj

Hoffman, J. (2015, 20 May). Constellations of trust and distrust in internet governance. Giganet: Global Internet Governance Academic Network, Annual Symposium. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2608414

Horwitz, J. (2013, July). After a lengthy battle, blackberry will finally let the indian government monitor its services. The Next Web. Retrieved from https://thenextweb.com/asia/2013/07/10/after-a-lengthy-battle-blackberry-will-finally-let-the-indian-government-monitor-its-servers/

Human Rights Council. (2016). Statement on the promotion, protection and enjoyment of human rights on the internet. A/HRC/32/L.20, 33rd Session of the Human Rights Council of the United Nations. Retrieved from http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/32/L.20

Hunton. (2014, 18 March). Outsourcers exempt from india's privacy regulations. Hunton Andrews Kurth Privacy and Information Security Law Blog. Retrieved from https://www.huntonprivacyblog.com/2011/08/articles/outsourcers-exempt-from-indias-privacy-regulations/

IAMAI. (2016, May). *Make in india: conducive policy and regulatory environment to incentivise data center infrastructure*. Internet and Mobile Association of India.

IBEF. (2018). It & ites industry in india. India Brand Equity Foundation. Retrieved from https://www.ibef.org/industry/information-technology-india.aspx

Jha, S. (2018, 23 May). Equalisation levy: 'google tax' revenue goes past rs 1,000 crore. Financial Express. Retrieved from https://www.financialexpress.com/economy/equalisation-levy-google-tax-revenue-goes-past-rs-1000-crore/1177595/

Justice KS Puttaswamy (Retd.) v. Union of India. (2017). WP (Civil) No. 494 of 2012, Supreme Court of India.

Kalra, A. (2018, 13 Oct). Us senators urge india to soften data localisation stance. Reuters. Retrieved from https://in.reuters.com/article/india-data-localisation/exclusive-u-s-senators-urge-india-to-soften-data-localisation-stance-idINKCN1MN0CJ

Kalra, A. & Shah, A. [Aditi]. (2018). U.s. tech giants plan to fight india's data localisation plans. Reuters, 20 August 2018.

Khamooshi, A. (2016, 21 March). Breaking down apple's iphone fight with the us government. The New York Times. Retrieved from https://www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html

Komaitis, K. (2017). The 'wicked problem' of data localisation. *Journal of Cyber Policy*. Retrieved from https://doi.org/10.1080/23738871.2017.1402942

Kostov, N. & Schechner, S. (2018). Google emerges as the early winner from europe′s new data privacy law. The Wall Street Journal. Retrieved from https://www.wsj.com/articles/%20eus-strict-new-privacy-law-is-sending-more-ad-money-to-google-1527759001

Kuner, C. (2015). Data nationalism and its discontents. 64 Emory Law Journal Online 2089. Retrieved from http://law.emory.edu/elj/elj-online/volume-64/responses/data-nationalism-its-discontents.html

LaRue, F. (2011). Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/17/27, 17th Session of the UN Human Rights Council. Retrieved from https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

Leviathan. (2015). *Quantifying the cost of forced localization*. Leviathan Security Group. Retrieved from https://tinyurl.com/y89q99yt

Macleod, J. (2015). *E-commerce and the wto: a developmental agenda*. GEG Africa.

Manyika, J., Lund, S., Bughin, J., Woetzel, J., Stamenov, K., & Dhingra, D. (2016, March). *Digital globalisation: the new era of global flows*. Mckinsey Global Institute.

MeITY. (2018). Software and services sector. Ministry of Electronics & Information Technology. Retrieved from http://meity.gov.in/content/software-and-services-sector

Ministry of Communications. (2011, 24 August). Clarification on information technology (reasonable security practices and procedures and sensitive personal data or information) rules, 2011 under section 43a of the information technology act, 2000. Press Information Bureau. Retrieved from http://pib.nic.in/newsite/erelcontent.aspx?relid=74990

Mohanty, B. & Srikumar, M. (August, 2017). Hitting refresh: making india-us data sharing work. ORF Special Report 39. Retrieved from https://www.orfonline.org/wp-content/uploads/2017/08/MLAT-Book.pdf

Necessary and Proportionate. (2014, May). The international principles on the application of human rights to communications surveillance. Necessary and Proportionate. Retrieved from https://necessaryandproportionate.org/principles

NITI Aayog. (2018, June). *Discussion paper on national strategy for artificial intelligence*. NITI Aayog. Retrieved from http://www.niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf

Nocetti, J. (2015, October). Russia's 'dictatorship of the law' approach to internet policy. Internet Policy Review, Vol. 4, Issue 4. Retrieved from https://policyreview.info/articles/analysis/russias-dictatorship-law-approach-internet-policy

OECD. (n.d.). Beps - frequently asked questions. Organisation for Economic Co-operation and Development. Retrieved from http://www.oecd.org/tax/beps/beps-frequentlyaskedquestions.htm#Action1

Pahwa, N. (2015, 25 March). Why s 69 a of the it act should have been changed by the supreme court. Medianama. Retrieved from https://www.medianama.com/2015/03/223-section-69-it-act-india/

Panday, J. (2016, 29 January). The internet has a new standard for censorship. The Wire.in. Retrieved from https://thewire.in/politics/the-internet-has-a-new-standard-for-censorship

Panday, J. (2017, August). E-commerce rcep chapter: have big tech's demands fizzled? Electronic Frontier Foundation. Retrieved from https://www.eff.org/deeplinks/2017/08/e-commerce-rcep-chapter-have-big-techs-demands-fizzled

Patnaik, S. (2018, 21 Mar). Taxing the digital economy: the rule of 'significant economic presence'. Cyril Amarchand Mangaldas Blog. Retrieved from https://tax.cyrilamarchandblogs.com/2018/03/taxing-digital-economy-rule-significant-economic-presence/

People's Union of Civil Liberties (PUCL) v. Union of India. (1996). AIR 1997 SC 568.

PhonePe. (2018, November). Data localization - why this kolaveri di? The Medium. Retrieved from https://blog.phonepe.com/data-localization-why-this-kolaveri-di-6d5680e3f012

Plaum, A. (2014, April). The impact of forced data localisation on fundamental rights. Access Now. Retrieved from https://www.thehindubusinessline.com/info-tech/social-media/centre-withdrawing-notification-on-social-media-hub-ag-informs-supreme-court/article24590834.ece

Press Trust of India. (2014, October). Vodafone secretly sharing data with british intelligence: home ministry. The Hindu. Retrieved from https://timesofindia.indiatimes.com/india/Vodafone-secretly-sharing-data-with-British-intelligence-Home-ministry/articleshow/31797862.cms/

Puttaswamy v. Union of India. (2017). 2017 (10) SCC 1, Supreme Court of India.

Roach, J. (2018). Under the sea, microsoft tests a datacenter that's quick to deploy, could provide internet connectivity for years. Microsoft. Retrieved from https://news.microsoft.com/features/under-the-sea-microsoft-tests-a-datacenter-thats-quick-to-deploy-could-provide-internet-connectivity-for-years/

Ruiz, D. (2018). Microsoft clears the air about fighting cloud act abuses. Electronic Frontier Foundation, September 14, 2018. Retrieved from https://www.eff.org/deeplinks/2018/09/microsoft-clears-air-about-fighting-cloud-act-abuses

Sargsyan, T. (2016). Data localisation and the role of infrastructure for surveillance, privacy and security. International Journal of Communication, Vol. 10, 2221-2237. Retrieved from ijoc.org/index.php/ijoc/article/viewFile/3854/1648

Secretary Ministry of Information and Broadcasting, Government of India v. Cricket Association of Bengal. (1995). 1995 AIR 1236.

Sehgal, M. (2018, 28 August). India-us likely to sign agreements on information security, geospatial cooperation. India Today. Retrieved from https://www.indiatoday.in/india/story/india-us-likely-to-sign-agreements-on-information-security-geospatial-cooperation-1325585-2018-08-28

Selby, J. (2017). Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both? *International Journal of Law and Information Technology*, *25*(3), 213–232. Retrieved from https://academic.oup.com/ijlit/article-abstract/25/3/213/3960261

Sentance, R. (2018, April). Freedom on the net 2017. GDPR: Which Websites are blocking visitors from the EU? Retrieved from https://www.econsultancy.com/blog/70065-gdpr-which-websites-are-blocking-visitors-from-the-eu-2

SFLC. (2014, March). Deity provides lists of sites blocked in 2013, but withholds orders! sflc.in. Retrieved from https://sflc.in/deity-provides-list-sites-blocked-2013-withholds-orders

SFLC. (2015, April). Deity says 2341 urls were blocked in 2014; refuses to reveal more. sflc.in. Retrieved from https://sflc.in/deity-says-2341-urls-were-blocked-2014-refuses-reveal-more

SFLC. (2018). Internet shutdowns - trends (january 2012 - april 2018). Software Freedom Law Centre, India. Retrieved from https://www.internetshutdowns.in/

Shah, A. [Ajay]. (2015). The economies of cloud computing: an indian perspective. The Leap Blog. Retrieved from https://blog.theleapjournal.org/2015/03/the-economics-of-cloud-computing-indian.html

Shah, A. [Ajay]. (2016, 31 January). Occam's razor of public policy. The Leap Blog. Retrieved from https://blog.theleapjournal.org/2016/01/occams-razor-of-public-policy.html

Shiv Cable v. State of Rajasthan. (1993). AIR 1993 Raj 197.

Shreya Singhal v. Union of India. (2015). AIR 2015 SC 1523.

Singh, S. (2012, April). No secrets on blackberry: govt gets its way on tapping popular messenger service. India Today, 7 April 2012. Retrieved from https://www.indiatoday.in/business/india/story/govt-to-tap-blackberry-messenger-security-privacy-98321-2012-04-07

Sinha, A. & Hickok, E. (2018). *Regulation of cross border transfers of personal data in asia*. Asian Business Law Institute. Retrieved from https://cis-india.org/internet-governance/files/dp-compendium

Sodan Singh v. New Delhi Municipal Corporation. (1988). AIR 1989 SC 1988.

Srikrishna Committee. (2018, 27 July). A free and fair digital economy: protecting privacy, empowering indians. Report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. Retrieved from http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

Srikumar, M. & Mohanty, B. (2018, August). The data protection bill is an opportunity to qualify for the cloud act. The Hindu.

State (N.C.T. Of Delhi) vs Navjot Sandhu. (2005). 2005 11 SCC 600.

The Economist. (2017, June). The world's most valuable resource is no longer oil, but data. Retrieved from https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

The Registrar (Judicial) vs Secretary. (2017). Madras High Court, Suo Motu W.P.(MD). No.16668 of 2017.

Thomas, T. K. (2014). National security council proposes 3-pronged plan to protect internet users. Hindu Businessline. Retrieved from https://tinyurl.com/ycdnp4qk

TRAI. (2017, 28 November). Recommendations on net neutrality. Telecom Regulatory Authority of India. Retrieved from https://www.trai.gov.in/sites/default/files/Recommendations_NN_2017_11_28.pdf

Unified License. (2014). License agreement for unified license. Department of Telecommunications. Retrieved from http://dot.gov.in/sites/default/files/Amended%5C%20UL%5C%20Agreement_0_1.pdf?download=1

United Nations Human Rights Council. (2012, June). The promotion, protection and enjoyment of human rights on the internet. UN Human Rights Council,

20th Session, Agenda Item 3, A/HRC/20/L.13. Retrieved from https://ap.ohchr.org/documents/E/HRC/d_res_dec/A_HRC_20_L13.doc

United Nations Human Rights Council. (2016, June). The promotion, protection and enjoyment of human rights on the internet. UN Human Rights Council, 32nd Session, Agenda Item 3, A/HRC/32/L.20. Retrieved from https://bit.ly/2QY3bY5

United States. (2016). Work programme on electronic commerce - non-paper from the united states. World Trade Organization. Retrieved from https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/JOBs/GC/94.pdf

United States. (2017). Communication from the united states: measures adopted and under development by china under its cyber security law. World Trade Organization. Retrieved from https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/S/C/W374.pdf

Ursic, H., Nurullaev, R., Cuevas, M. O., & Szulewski, P. (2018, 29 January). Data localisation measures and their impacts on data science. Handbook on Data Science and the Law, Edward Elgar (forthcoming). Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102890

Wattal Committee. (2016, December). Medium term recommendations to strengthen digital payments ecosystem. Department of Economic Affairs, Ministry of Finance.

Wikipedia. (2016, 14 November). Internet censorship in india. Wikipedia. Retrieved from https://tinyurl.com/y94t5lrs

Zittrain, J. (1974). The generative internet. Harvard Library, Office for Scholarly Communication. Retrieved from http://nrs.harvard.edu/urn-3:HUL.InstRepos:9385626