US·INDIA
STRATEGIC PARTNERSHIP FORUM

November 6, 2017

Shri Arvind Kumar
Advisor (BB&PA)
Telecom Regulatory Authority of India

Subject: USISPF Response to TRAI Consultation Paper on Privacy, Security and Ownership of Data in the Telecom Sector

Dear Sir,

Greeting from U.S. India Strategic Partnership Forum (USISPF), a non-profit organization focused on strengthening business relations between the U.S. and India, and enhancing the U.S.-India strategic relationship. We are committed to creating the most powerful strategic partnership between the two countries. Promoting bilateral trade is an important part of USISPF's work, but USISPF's mission reaches far beyond this. We believe it is about business and government coming together in new ways to create meaningful opportunities that have the power to change the lives of citizens. USISPF is headquartered in Washington DC, with offices in New York, Silicon Valley, Delhi and Mumbai.

I am writing to you in response to the Consultation Paper on Privacy, Security and Ownership of Data in the Telecom Sector released by TRAI on 9th August 2017. Our detailed responses to the questions that the Consultation Paper raises have been attached as Annexure.

Close collaboration between government and industry is critical to realize India's digital potential, and we are keen to support you in this endeavour. Feel free to contact me or my Technology, Media & Telecom Lead, Ms. Shagufta Kamran in New Delhi at skamran@usispf.org or +91 9999107923.

Once again, we thank you and your colleagues at TRAI for providing the opportunity to comment. We look forward to our continued partnership on all issues impacting the growth of India's digital economy.

Sincerely,

Mukesh Aghi
President
US India Strategic Partnership Forum

ANNEXURE: USISPF RESPONSE TO TRAI CONSULTATION PAPER ON PRIVACY, SECURITY AND OWNERSHIP OF DATA IN THE TELECOM SECTOR

Question 1: Are the data protection requirements currently applicable to all the players in the eco-system in India sufficient to protect the interests of telecom subscribers? What are the additional measures, if any, that need to be considered in this regard?

There is a need to differentiate between data protection for 'telco subscribers,' who use the licensed services directly from the telcos/ Internet service providers (ISPs), and the users of unlicensed services (which could be provided by the telco itself), including apps that are delivered over the telecom/Internet infrastructure that would are customers of non-telco entities. For the licensed services, telco subscribers are provided protection under the Indian Telegraph Act and the licensing agreement. For the unlicensed services, the users are protected through the Information Technology Act (IT Act) and related rules covering protection of sensitive personal information, in addition to generic laws covering matters of contractual relationship between a service provider and a user, which also apply to telcos and licensed services.

Having a technology/platform neutral data protection law which applies horizontally across the ecosystem should be the path forward. The Ministry of IT is already working to draft a comprehensive data protection law that would cover all the sectors and bring uniformity. While drafting this law, it is important to take into account the socio-economic impact of Internet-enabled services and apps and data driven innovation. A recent study[1] by ICRIER estimates that apps contributed a minimum of USD 20.4 billion in the year 2015-16 to India's GDP, and this contribution is expected to grow to USD 270.9 billion by 2020.This would be nearly eight percent of India's GDP. A report[2] by Analysys Mason estimates that data driven innovation contributed USD 10 billion to India's Gross Value Added (GVA) in 2015 and this contribution is expected to rise to USD 50 billion by 2020.

It is important to empower the users without over-regulating the data controllers or data collection. Multiple studies suggest that restrictive frameworks have negative impact on the economy. As has been estimated by the Information Technology and Innovation Foundation, with the European Union's (EU) 'cookie notification law', around USD 2.3 billion per year were burdened on consumers without benefits in the same proportion[3].

The public policy focus should focus on providing regulatory certainty and consistency, preventing harm to users, misuse of personal information and making companies accountable through self-regulation without being prescriptive. The framework should recognize the market/industry driven developments have led to an increase in user transparency and trust.

[1] http://icrier.org/pdf/Estimating_eValue_of_Internet%20Based%20Applications.pdf
[2] http://report.analysysmason.com/DDI_Emerging_APAC/DDI%20in%20emerging%20APAC%20-%20Final%20report%20-%202016%2008%2006%20-%20FINAL.pdf
[3] Daniel Castro and Alan McQuinn, The Economic Costs of the European Union's Cookie Notification Policy, Information Technology and Innovation Foundation, November 2014: www2.itif.org/2014-economic-costs-eu-cookie.pdf.

Further, building capacity of users through education and awareness and strengthening grievance redressal would be important considerations.

Question 2: In light of recent advances in technology, what changes, if any, are recommended to the definition of personal data? Should the User's consent be taken before sharing his/her personal data for commercial purposes? What are the measures that should be considered in order to empower users to own and take control of his/her personal data? In particular, what are the new capabilities that must be granted to consumers over the use of their Personal data?

Definition of Personal Data

Indian definition of 'personal information' – found in rule 2(1)(h), SPDI Rules – covers both information which can be used directly and indirectly to identify a person. This classification of personal data is also recognised by the United States, most European countries, Australia, Singapore, Japan, and others. The Indian definition is broad enough to cover changes due to technological advancements.

It should however, as recognized by the Supreme Court of India, apply to various contexts and be applied proportionally. Proportionality means that the appropriate level of protection is applied to different kinds of information. For instance, the debate on financial information as sensitive personal information is a good example. While such transactional data may be personal to the user, it is also business information of the company making the financial transaction, and may assist the company in determining the user's potential and in offering her more focused services. Imposing additional emphasis on consent, restricts the growth of businesses especially in areas where the business may not have foreseen while taking consent.

Further, consent may not be appropriate in certain contexts, such as in fraud prevention or in protecting network security, or where it is impracticable or impossible to obtain direct consent (for example, in the context of machine learning or with the Internet of Things).

It is also important to note that a number of countries either do not rely on consent as the legal basis of processing of personal data, or are creating additional legal basis for the processing of personal data. For example, several jurisdictions (such as Australia[4], New Zealand[5] and Japan[6]) permit the collection of personal data with notification of purpose in the absence of consent. Singapore is also proposing to permit the collection and use of personal data on the basis of notifying individuals of the purpose of the processing of personal data[7].

User's Consent

SPDI Rules already provide for a consent-based model for handling personal data, including collecting, disclosing and transferring it. Users must be provided privacy policies explaining

[4] Australia Privacy Act, APP 3 and 5
[5] New Zealand Privacy Act, Principles 2 and 3
[6] Japan Act on the Protection of Personal Information, Article 18
[7] Singapore Public Consultation for Approaches to Managing Personal Data in the Digital Economy

how their data will be used, and also names of people responsible for their personal data. Consent under contract laws of India has to be free, and without undue influence or misrepresentation.

Further, it is important to ensure that too many consent-related privacy choices and requests to collect data should not be mandated. Mandating so can lead to individuals feeling interrupted or overwhelmed, and spoiling the user experience. For instance, users may also not like to provide consent for every transaction as it may adversely impact user experience and introduce latency in the transactional flow.

Therefore, it is important to let companies use "legitimate interest" as a legal ground for data processing. This is a valid ground in many jurisdictions, and enables companies to collect data that is necessary to support, deliver and improve a variety of services for the benefit of users, data controllers or the society.

We encourage the government to create a flexible approach to consent so as to ensure an efficient user experience while ensuring appropriate protections for data subjects. A risk-based approach to consent, that is the standards for consent for use of customer account information will differ from the standards for consent with regard to biometric information. A one-size-fits-all framework for consent does not work. Further, prescriptive legal requirements will constrain a company's ability to adapt its services (and correspondingly, its privacy policy) to enable new services, features or devices. Consent should enable the collection and use of data based on a privacy policy that is suited to the context, and is clear, transparent and reasonable. Beyond a basic set of controls, it should be left to the company in an agreement with the customer to determine the appropriate terms for consent. Enforcement should focus on ensuring that a company adheres to its own policy.

User Empowerment

Given that privacy means different things to different users, it is important to put users in control by providing the necessary information and options to exercise their choice meaningfully wherever relevant. For instance, the Android OS platform empowers users to grant granular permissions to the apps they install on their devices through the Play store. Through easy to navigate settings, users can change these permissions anytime. To enhance user transparency and trust, many companies provide 'one stop shop' privacy help center, easy to understand privacy notices, single view of what PI is collected and processed by the company.

Additionally, some companies are empowering users by providing data portability, allowing users to download their data from the platforms they use, even potentially moving their data to competing platforms. Data portability and interoperability help users avoid feeling locked-into any service, and give them the freedom to seek the products that work best for them. The law should recognize these market/industry driven developments that have led to increase in user transparency and trust.

Question 3: What should be the Rights and Responsibilities of the Data Controllers? Can the Rights of Data Controller supersede the Rights of an Individual over his/her Personal Data? Suggest a mechanism for regulating and governing the Data Controllers.

The SPDI Rules already provide for the rights and responsibilities of data controllers. They are to give users notice of privacy practices; to seek informed consent; not collect more personal data than is required; to seek consent before disclosing personal data; to make personal data available to the users; to handle data securely and to handle sensitive personal data with additional protections.

There is no dichotomy between rights of data controllers and individuals, so the question of one superseding the other does not arise. To make data driven innovation compatible with data privacy, it is critical to empower the users, without over-regulating the data controllers or data collection.

APEC Privacy Framework[8] is a business friendly and user centric framework which also supports cross border data flows and should be considered when formulating the law. It recommends privacy principles of Preventing Harm, Notice, Collection Limitations, Uses of Personal Information, Choice, Integrity of Personal Information, Security Safeguards, Access & Correction and Accountability. These principles are informed by the Fair Information Practice Principles (FIPPs) and the OECD principles and were drafted with the digital economy in mind.

Instead of prescribing privacy practices in form of administrative requirements, the privacy framework should define the broad principles and requirements and allow organizations to design their own privacy programs that could be based on due diligence guidelines. While organizations should be allowed to self-regulate, they should be held accountable for any violations. In case of any breach or complaint, the onus to prove due diligence should lie with the organizations.

Here it is also important to note that the distinction between data controllers, which determine the means and purposes of processing data and data processors, which process the data on behalf of another organization is preserved. Privacy obligations (including grievance redressal) should primarily rest upon the former. Data processors merely processing data on behalf of data controllers are responsible for following the data controllers' instructions and assisting them in meeting their obligations. If the fault of an organisation processing data within an ecosystem can be demonstrated, liability should accordingly be imputed.

The 'controller-processor' relationships are governed through contractual means and there should be no unreasonable intervention in these relationships. It is important to note that the Indian IT industry (acting as data processors) has been negatively impacted due to restrictions to the transfer of data under the EU Data Protection Regime. Also, the rules issued under Section 43A of the Information Technology Act did not make a distinction between controller and processor and this led to lot of confusion and backlash. To address industry concerns, the government later issued a clarification[9] which helped create the desired distinction and exempted processors from certain requirements.

[8] http://publications.apec.org/publication-detail.php?pub_id=390
[9] https://www.dsci.in/sites/default/files/Government%20Clarification%20on%20notified%20Rules%20under%20sec%2043A%20of%20IT%20(Amendment)%20Act%202008.pdf

Question 4: Given the fears related to abuse of this data, is it advisable to create a technology enabled architecture to audit the use of personal data, and associated consent? Will an audit-based mechanism provide sufficient visibility for the government or its authorized authority to prevent harm? Can the industry create a sufficiently capable workforce of auditors who can take on these responsibilities?

Given the scale and volume of transactions happening on the Internet every second and multiple players involved in each transaction, it may not be practically possible to create a centralized ex *ante* tech based compliance system. It is recommended that policy responses focus on building understanding among users through education and awareness, making organizations accountable through self-regulation and strengthening grievance redressal.

A suggested approach would involve evaluating the risk of harms (negative impact on personal data and privacy) through empirical exercises and taking measures to mitigate those risks (rather than weighing 'fears'). Industry could help the government understand the risks and benefits of technology solutions, business decisions and the impact of particular prospective regulatory paths and suggest that government make such decisions based on empirical information.

A self-regulatory approach backed by co-regulation, seals and certifications, where necessary is the preferred way forward. This way, organisation can focus on high-risk data uses to minimise abuse, and monitor low-risk situations such as B2B data processing or other common and everyday uses of data.

Question 5: What, if any, are the measures that must be taken to encourage the creation of new data based businesses consistent with the overall framework of data protection?

The interests of consumers are important in any measures taken by the government. At the same time, the government should promote businesses without sacrificing consumer interests. The government's role in a free market economy like ours is to balance regulation with freedom of trade. The government's role by way of regulation should, therefore, be to prevent harm and promote security in the market, without over-regulating.

The best interest of the consumer is served when there is thriving competition in the market. In the present context, data analytics, behavioural analysis, aggregation and anonymization are the best techniques for improving services and user experience. Such techniques are enhanced when companies devote sufficient resources to research and development and focus on innovation.

Further, legislation must necessarily be supported by an adequate implementation ecosystem, including institutional capacities and capabilities, industry self-regulation, effective grievance redressal system, user awareness, active civil society, and research. Therefore, privacy framework should be outcome driven and focus on building the necessary ecosystem.

Question 6: Should government or its authorized authority setup a data sandbox, which allows the regulated companies to create anonymized data sets which can be used for the development of newer services?

In a technology-based and innovation-driven ecosystem, development of new services does not require regulation and incentivised provision of data sets by the government. As India moves towards being a data-rich country[10], such move may not be required either. The focus should instead be on improving access to the Internet and encouraging more and more people to become part of the ecosystem.

Moreover, any steps by the government to create such a sandbox would also be against the constitutional right to property (Article 300A) under which the state cannot deprive someone of their private property except by statute. Data, particularly that protected under copyright law, amounts to property, by way of a combined reading of Indian copyright law and Supreme Court's judgment in the *Super Cassette* case (2008)[11]. Anonymised datasets, therefore, would also be covered by property rights, and would be constitutionally protected.

Even if such datasets were lawfully acquired under statute, but forced to be taken away from companies, such action would *prima facie* implicate the fundamental right to trade under Article 19(1)(g) of the Constitution. Big data businesses with Indian subsidiaries have introduced their proprietary know-how and technologies to the Indian market along with huge investments, bringing great benefits to consumers, and have complied with Indian law. It is imperative upon the regulator and the government to respect their rights under Indian law, based on which they reposed their trust in the Indian market.

Data is an important asset which is utilized by businesses to create useful products. However, the value is not intrinsic to the data itself but to the insights derived from that data. Ideas continue to matter more than data. In addition, data is a non-rivalrous and non -exclusive resource - many companies have access to the same data. Several experts and researchers have argued that data is just one input of many in the process of innovation and market success is not a barrier to entry[12]. There have been several startups in the recent past that have become successful – Examples: Tinder — an online dating app that launched less than 3 years ago — is adding a million users a week and is already valued at over $1 billion. Similarly, the food startup Zomato is India's first e-commerce unicorn to break even, and is headed for profitability[13].

Question 7: How can the government or its authorized authority setup a technology solution that can assist it in monitoring the ecosystem for compliance? What are the attributes of such a solution that allow the regulations to keep pace with a changing technology ecosystem?

[10] Nandan Nilekani, India Must Embrace Data Democracy, 2017: http://carnegieendowment.org/files/Data_Democracy%2016th%20Aug%20Presenting.pdf
[11] Entertainment Network (India) Ltd v. Super Cassette Industries Ltd, (2008) 9 SCR 165.
[12] http://www.project-disco.org/competition/040215-big-data-entry-barrier-tinder-can-tell-us/#.WZqyFJMjFE6
[13] https://www.forbes.com/sites/saritharai/2016/02/08/food-startup-zomato-is-indias-first-unicorn-to-break-even-headed-for-profitability-by-mid-2016/#205713344ba8

Technology developments are so dynamic that attempting to monitor for compliance will likely place significant, if not overwhelming, burden on a government owned and operated tech enabled compliance system. Additionally, this is likely to raise privacy concerns as it installs a system of government monitoring and surveillance. Industry is best placed to comply with the privacy principles under a self-regulatory framework and putting users in control is critical.

Instead of government monitoring, the legislator should be encouraged to recognize and endorse a culture of corporate accountability, that would limit the ex *ante* enforcement approach to a minimum. This has been the approach of other privacy enforcement authorities who have seen how effective privacy and data protection are better achieved by incentivizing companies to adopt best practices and demonstrate that they are accountable to their users. This approach, which is compatible with effective enforcement, constitutes the essence of the APEC Cross Border Privacy Rules[14] (CBPRs) regime. For further information on essential mechanisms for enabling cross border data transfers, the "White Paper on Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy"[15] provides a good reference.

Question 8: What are the measures that should be considered in order to strengthen and preserve the safety and security of telecommunications infrastructure and the digital ecosystem as a whole?

Regulations on encryption, which plays a vital role in security of the digital ecosystem, have irregularities in India. Levels of encryption are prescribed differently by different authorities, which causes ambiguity. For e.g., Indian ISPs must have 40-bit encryption keys, which is a relatively low standard. There is no such restriction on third-parties, including OTTs. RBI and SEBI, on the other hand, stipulate the use of longer encryption keys for certain purposes, causing different standards to exist for different purposes.

Moreover, there is an urgent need to issue rules to govern encryption under section 84A of the IT Act which is aimed at promoting stronger encryption. This assumes even more relevance with telecommunications being declared as 'critical information infrastructure'.

Strong encryption needs to be encouraged through government policy, wherever possible. Additionally, harmonisation of encryption regulations, issuance of rules under the IT Act for strong encryption, and encouragement to Indian businesses to make strongly encrypted products to compete in global markets would go a long way to strengthen and preserve safety and security of the digital ecosystem.

Question 9: What are the key issues of data protection pertaining to the collection and use of data by various other stakeholders in the digital ecosystem, including content and application service providers, device manufacturers, operating systems, browsers, etc? What mechanisms need to be put in place in order to address these issues?

[14] http://www.cbprs.org/
[15] Centre for Information Policy Leadership
https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper__final__-_essential_legislative_approaches_for_enabling_cross-border_data_transfers.pdf

Every data controller should be responsible for protecting the privacy of its users under the proposed legal framework. Breaking down the ecosystem to understand issues at various levels may be a good approach but having a technology/platform neutral data protection law which applies horizontally across the ecosystem should be the way forward.

Also, it is important to recognize the market forces within different categories which are driving development of features that enhance privacy and provide more choices to users. For e.g. many browsers today provide incognito mode, do not track features to users; similarly App permissions on Android can easily be controlled by the users.

Question 10: Is there a need for bringing about greater parity in the data protection norms applicable to TSPs and other communication service providers offering comparable services (such as Internet based voice and messaging services). What are the various options that may be considered in this regard?

TSPs control the telecom infrastructure, which has few competitors and high barriers to entry. OTTs, on the other hand, face a highly fluid consumer preference with numerous competitors owing to low barriers to entry, and also lack control on the infrastructure. Owing to controlling the infrastructure, TSPs enjoy regulatory protection and incentives which OTTs do not. Examples include the right to obtain numbering resources, interconnect with the PSTN, or own spectrum.

Having a technology/platform neutral data protection law which applies horizontally across the ecosystem should be the path forward. The Ministry of IT is already working to draft a comprehensive data protection law that would cover all the sectors and bring uniformity. While drafting this law, it is important to take into account the socio-economic impact of Internet-enabled services and apps and data driven innovation.

Once the data protection law is enacted, TRAI should review the existing provisions in the Indian Telegraph Act and licensing conditions to recommend changes to the Department of Telecommunications (DoT) to align with the new requirements. DoT/TRAI could also issue advisory or guidelines for the telcos to comply with these new requirements.

Question 11: What should be the legitimate exceptions to the data protection requirements imposed on TSPs and other providers in the digital ecosystem and how should these be designed? In particular, what are the checks and balances that need to be considered in the context of lawful surveillance and law enforcement requirements?

Encryption: A strong encryption regime is must and cannot be overemphasised. Most data controllers comply with legally valid requests for user data in various jurisdictions, and recognise the government's duty to protect national security and public safety.

The advantages of encryption include protection protects against malicious actors, hostile countries, foreign intelligence agencies, and cyber criminals. Any attempts to introduce deliberate backdoors in encryption technology harms the fundamental security afforded to it.

Moreover, strong encryption provides a competitive market edge, which the government should promote (including the use of strong encryption) to enable Indian companies to compete in privacy-conscious markets.

Anonymized and de-identified data: Given that lot of economic value of data today is generated through processing of anonymized and de-identified data, the government should incentivize the processing of such data over personal data where appropriate. While anonymized data should be kept out of scope of the law, for de-identified data, at a minimum, there should be reasonable exemptions. Singapore and Japan provide a good reference point when it comes to dealing with anonymized data.

Question 12: What are the measures that can be considered in order to address the potential issues arising from cross border flow of information and jurisdictional challenges in the digital ecosystem?

There are three main reasons in support of the cross-border flow of information:

- Access to information is an international human right.
- Internet access and cross-border data flows comprise and enable international trade and are therefore subject to international trade laws and norms, the main ones being non-discrimination and transparency.
- All major international data protection instruments recognize the need to facilitate the free flow of data, including personal data.

Globalization and technology have made cross border data flows ubiquitous and an essential phenomenon for economic activity globally. The growth of the Internet and the ability to move data rapidly globally has been a key building block of the global economic order and this is relevant for companies that act as controllers and those who act on their behalf. Cross-border data flows have allowed business to communicate customer orders in real-time, make quick decisions about manufacturing loads and rapidly tweak designs in response to shifts in consumer desires. This has enabled the disaggregation by businesses of their supply chains across countries. In fact, there is no international data protection and privacy instrument that does not recognize the need to ensure that data can flow both domestically and internationally.

Any disruption/hindrances to cross border data flows, would adversely impact innovation, economic competitiveness and availability of technology and services to users. Cloud computing, for instance, is affordable for small businesses and startups because it relies on massive economies of scale with globally distributed datacenters. A 2014 ECIPE study[16] had estimated that 'if India were to introduce an economy-wide data localisation measure, the effect on GDP would be -0.8%. In addition, the domestic and foreign direct investments (FDI) that drive Indian exports and long-term growth, would drop by -1.9%. In terms of welfare loss, data localisation would cost the Indian worker almost 11 percent of one average month's salary.'

[16] http://www.ecipe.org/app/uploads/2014/12/ECIPE_bulletin814_dataloc_india.pdf

Data access should be aimed to be secured by improving the international framework, so as to enable the Indian government to access data from foreign, chiefly American, providers. As an illustration, the 'Framework for the U.S.-India Cyber Relationship' released in 2016 contains a commitment to "sharing information on a real time or near real time basis, when practical and consistent with existing bilateral arrangements, about malicious cybersecurity threats, attacks and activities, and establishing appropriate mechanisms to improve such information sharing."[17] Newer agreements between governments are required where Indian law enforcement authorities could seek content from foreign companies directly (outside of the MLAT process).

Justice A P Shah Committee also recognised Technological Neutrality and Interoperability with International Standards as one of the five salient features, and recommended that any proposed framework for privacy must be technologically neutral and interoperable with international standards. In particular, the Committee called for harmonization of the right to privacy with multiple international regimes, create trust and facilitate cooperation between national and international stakeholders and provide equal and adequate levels of protection to data processed inside India as well as outside it.

Rather than focusing efforts around data localization provisions that are hard to implement and enforce, it is important that users are better served by providing a regulatory framework for international data transfers that sets adequate guarantees to users' data but does not restrict or prohibit the data flows from the outset. Given below are some detailed observations pertaining to data flows that should be considered when designing India's data transfer framework:

- Pragmatic arrangements like APEC Cross Border Privacy Rules[18] (CBPRs) which are based on mutual recognition, accountability and commonly applicable privacy principles that enable efficient cross border data flows without unnecessary administrative burdens are a preferred model. The Indian government should consider becoming a member of such arrangements as this will help in enhancing market access for Indian companies especially the IT industry. APEC economies like the US, Canada, Mexico, Japan and Korea have started using this mechanism.
- Contractual freedom should be preserved in B2B data flows across jurisdictions
- Forced data localization should be rejected as it is incapable of achieving the objectives behind these measures, whether economic, security or access to data for law enforcement purposes.
- Requiring data centers to be located domestically undermines the cost-effectiveness of cloud-based computing services
- Law Enforcement - There is growing frustration among governments and law enforcement agencies when it comes to accessing data residing in foreign jurisdictions. The MLAT process is broken and needs to be reformed to enable efficient sharing of data between companies based out of foreign jurisdictions and Indian law enforcement agencies. The law enforcement requests for digital evidence should be based on the location and nationality of users, not the location of data.

[17] Framework for the U.S.-India Cyber Relationship, United States Embassy: https://in.usembassy.gov/framework-u-s-india-cyber-relationship/.
[18] http://www.cbprs.org/

While working on reforming the MLAT process, the Indian government should work with the US government to develop a UK-US type agreement. This would require legislative changes on both sides including enhancing privacy standards on the Indian side for legally accessing data. Indian think tank ORF recently published a study[19] on India-US data sharing. The Indian government should consider the recommendations of this study.

- Security: Some believe that storing data in the local jurisdiction enhances security. This is a misconception as storing data across jurisdictions actually increases security and reliability and is helpful in business continuity during disasters. Storing data in one location (through data localization measures) makes data more vulnerable.
    - Technical security expertise is expensive and rare. Companies have invested hundreds of millions of dollars ensuring that their data centers are secure. Attackers and criminals can more easily overwhelm a less sophisticated server or network.
    - If there is a technical failure or natural disaster, when one data center goes down, another can take over, ensuring that service isn't interrupted.
    - Local data storage is more vulnerable to attacks because they are generally harder to update with the latest security software.

[19] http://cf.orfonline.org/wp-content/uploads/2017/08/ORF_SpecialReport_39_DataSharing.pdf