November 6, 2017

To,

1. Shri R.S. Sharma
   Chairman
   Telecom Regulatory Authority of India (TRAI)
   New Delhi

2. Shri Arvind Kumar
   Advisor (Broadband and Policy Analysis)
   Telecom Regulatory Authority of India (TRAI)
   New Delhi

3. Shri Bharat Gupta
   Joint Advisor
   Telecom Regulatory Authority of India (TRAI)
   New Delhi

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

About us

Koan Advisory Group is a New Delhi based policy advisory firm, which combines thorough domain knowledge across multiple technology oriented sectors with continuous engagement of decision makers in industry and government. We have previously engaged with various regulatory arms, including TRAI on issues related to telecommunications and future policy making.

Submission

We laud this initiative of the TRAI to onboard public comments to inform its recommendations regarding India's revised data protection framework. In many ways, data will form the basis of the Fourth Industrial Revolution and therefore, the new digital economy rests on three key aspects: user control over their data, trust reposed in the service provider handling the information, and innovative use of the data by technology companies. Importantly, as data-driven innovation becomes the norm, it is important data protection frameworks remain innovative, to keep abreast with technologies. At the same time, it is also imperative that our data protection frameworks adequately protect the rights and interests of consumers, who have a tangible interest in the manner in which their data is protected.

Thus, it is essential that the technology community and decision makers ask the question - should data protection be intrinsic to the technology, such as based on privacy by design, or exogenous mechanisms like strict regulation? Most jurisdictions, including India, have already tried the latter approach. While regulation has been successful to an extent, it has largely been limited to cases where data breaches or other violations have caused tangible damage. However, owing to the inherently intangible nature of data and its movement, it has and will continue to become harder to meaningfully

implement regulations and adequately protect consumers. Further, considering growth of start-ups in India and the Government's focus on creating an innovation hub in India it is imperative that cost of compliance is rationalized with this objective. Thus, it may be time for India to lead the way in adopting a technological approach for data protection.

It should be pointed out at the outset, that while formulating a data protection framework for India, it is important that we take into account the composition of the data driven business landscape within India – indigenous start-ups, larger overseas service providers, indigenous competitors to the overseas service providers. The European Union, which is a model jurisdiction for data protection, must be differentiated as against the Indian context, where smaller businesses cannot sustain highly onerous obligations as under the General Data Protection Rules (GDPR).

India's extant data protection framework is summarized hereunder for convenience:

i. TRAI's regulatory mandate extends to the telecommunications sector which encompasses internet and other network service providers. While confidentiality and security of information carried over networks must be in accordance with the provisions of the Telegraph Act and the license conditions of service providers, the Information Technology Act, 2000 (IT Act) contains provisions governing data across mediums. However, as things stand today, the major onus for ensuring security of information lies with the telecommunication network provider. A general data protection law, covering all manner of data and mediums used should be principle based and allocate accountability wherever necessary. The nodal Ministry under the IT Act - the Ministry of Electronics and Information Technology (MeitY) has set up a Committee, under Justice B N Srikrishna, to look into the issue and is expected to provide the required general data protection framework before the end of the year. Since the Meity Committee has limited stakeholder representation, it is hoped that the TRAI will nuance the discussion by providing stakeholder feedback to the Meity Committee.

ii. The Supreme Court of India has recognised the right to privacy as a fundamental right under the right to life under Article 21 of the Constitution[1] - while the majority identified 'informational privacy' as a facet of the right to privacy, it left the specifics to be decided by the Meity Committee. Some individual Judges, such as Justice Kaul, detailed aspects of an appropriate data protection regime. In this context, it has delineated that the State must ensure that information is not used without the consent of users, and that it is used for the purpose and to the extent it was disclosed.

iii. The AP Shah Committee submitted its report on Privacy Principles in 2012. While the Report focussed on State surveillance, it also identified weaknesses within the extant data protection regime and recognised privacy by design as an aspect of the principle of accountability.

<u>Question 1</u>

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?

The current requirements under the data protection laws are inadequate in protecting the interests of telecom subscribers.

[1] *Justice KS Puttuswamy & Anr. v Union of India & Ors*. WP (Civil) No. 494 of 2012 in the Supreme Court of India.

The current data protection requirements for telecom operators only extend to specific interception provisions under the Telegraph Act, 1885, and the license conditions for licensed telecommunication service providers. Further, under the Information Technology Act, 2000, personal information, which is information capable of identifying an individual[2] is broadly protected by way of criminal penalties. These criminal penalties also extend to data disclosures in breach of contract. Further, the Act provides civil remedies to the data subject against a body corporate which fails to undertake reasonable security practices in handling *sensitive personal data or information* ("SPDI").[3] SPDI has been defined under an exhaustive list as:

i. financial Information,
ii. passwords,
iii. physical, physiological and mental health condition,
iv. medical records and history,
v. bio-metric information,
vi. any other detail or information provided to body corporate for providing services,
vii. any such information received or held under contract.[4]

Under the Rules framed under the Act, companies which, on their own, or on behalf of another collects, receives, possess, stores, deals or handles information of a provider are required to provide a policy for privacy and disclosure of information. With respect to collection of information, the Rules specify the requirement of notification and consent for SPDI. Further, the information so obtained cannot be retained longer than required for the purpose for which it was collected, and must be used only for those purposes. Disclosure of the information to third parties requires either prior permission under a contract or that such disclosure is necessary for complying with a legal obligation. Transfer of SPDI to another country requires that the same level of data protection requirements is adhered to and that a contractual provision or consent for such transfer has been obtained.

While the rules are in line with the broader data protection principles found across jurisdictions, they are inadequate, firstly in addressing accountability, and secondly in defining their scope of application. Furthermore, given the changes in technology and application of data, newer issues regarding data collection and processing, such as big data analytics, internet of things (IoT) and artificial intelligence (AI), pose renewed challenges for the management and protection of data. As data collection is becoming increasingly based on open flows of information which take place in real time, data protection laws need to be updated to reflect this new market paradigm.

While the right to privacy is not of an absolute nature, good data protection laws tend to follow principles espoused by authors such as Daniel J Solove. He has advocated treating the right to privacy and related policies on harms based models, which prioritise resolving more pernicious harms as opposed to comparatively benign ones.

Under a risk-based framework for data protection, data processing is categorised as per the potential risk of harm associated with the processing activity. Under the EU GDPR, data processing activities are categorised *as high risk; risk;* or *low risk*; with data protection obligations varying in accordance with the level of risk. The assessment and classification of the activity according to the different risk profiles

[2] See Rule 2(1)(i) of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

[3] Section 43A, Information Technology Act, 2000.

[4] See Rule 3 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

is to be done by the organisation processing the data, according to general guidelines provided by the GDPR.

A similar harm-based framework is advisable for India as well, wherein stringent notice and consent mechanisms, that currently exist for all categories of SPDI, may be required for high risk activities. However, it needs to be kept in mind that such a framework needs clear guiding principles with respect to risk assessment. Additionally, such risk assessment exercises can be highly cumbersome for smaller businesses, which cannot engage the requisite technical, institutional and economic resources for the same. Thus, regulatory frameworks should be focused on addressing these challenges through capacity building exercises as well as creation of resource centres for ready availability of such information.

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?

Personal Data

While personal data is defined in terms of whether the data can identify a person, such criterion does not adequately cover the evolved manner in which personal information is collected. Big data analytics, for instance, relies heavily on anonymised data that does not directly identify individuals. In this context, while anonymised data may be accorded simpler, less stringent privacy protections, it must be borne in mind that complete anonymization is not achievable. The onset of machine learning capabilities has demonstrated that anonymised data can in fact be re-identified easily. Thus, sufficient safeguards in the form of anonymization guidelines and standards are necessary if such a distinction is created including the prohibition of de-anonymization subject to stringent penalization.

User Consent

While user consent continues to remain the legal basis for processing personal data, it is not meaningful where individuals may lose the service they desire by refusing consenting to divulge personal data essential to providing the service, or where such denial of consent for processing in effect exposes the user to further vulnerabilities. In such a situation, processing should be based on alternatives like legitimate interests, performance of contract and processing to protect the interests of the data subject, or where the processing is necessary for compliance with a legal obligation to which the organisation is subject. Importantly, facilitating privacy by design ensures that users have greater control over their data.

At present, user consent is a blanket requirement for the collection of SPDI. This should be further nuanced to require the obtainment of user consent only for high risk data, while reasonable exceptions along the lines of legitimate interests and other processing events highlighted above should further clarify consent as the legal basis of processing. Several jurisdictions (such as Australia[5],

[5] Australia Privacy Act, APP 3 and 5

New Zealand[6] and Japan[7]) 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[8].

Enhancing user control over personal data

Consumers must be recognised as an essential part of the data collection process. This necessitates the need for addressing consumer ignorance regarding the exact significance of the data that they share in lieu of obtaining services. Thus, users must be made aware of the monetary value of their data, and also the risks associated with sharing certain data on their rights and obligations. This will contribute to a smarter digital economy wherein, the demand for optimally secure and private services is actively sourced from consumer, thus incentivising businesses to differentiate their products on the basis of better privacy controls.

The Supreme Court has further recognised that an individual has the right to control one's life when providing personal data for various facilities and services, and so it is essential that the individual has the knowledge of the use of the data, as well as the ability to correct and amend it.[9] This is especially relevant in light of algorithm-based determinism, that can often lead to discriminatory inferences regarding individuals. Thus, the right to transparency, whereby an individual is aware of the information being collected, and the right to rectification are seminal to an effective data protection framework that recognises the value of an individual's privacy rights. The AP Shah Principles provide further guidance, where they specifically lay down the significance of horizontal applicability of data protection rules across sectors, including the government.

Innovative technologies can further be leveraged to enhance user control. For instance, distributed ledger technologies which incorporate decentralised systems of interaction, allow the user to retain confidential data, thereby eliminating the need for such disclosures as a precondition for availing of a service. Incentivising new services based on such technological advancements can further facilitate enhanced user control over data.

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.

At the very outset, data controllers and data processors should be differentiated as per the processing activity engaged in. While data controllers determine the purpose for which data is to be collected, the processor is required to carry out the processing activity as per the requirements stipulated by the data controller. The rights and responsibilities of data controllers and data processors are in effect determined by the contractual arrangements between the controller and the processor, as well as the contractual arrangements between the data subject and the data controller. Broad guidelines based on the principles of accountability, minimisation, purpose and collection limitation, as also identified

[6] New Zealand Privacy Act, Principles 2 and 3

[7] Japan Act on the Protection of Personal Information, Article 18

[8] Singapore Public Consultation for Approaches to Managing Personal Data in the Digital Economy

[9] Justice Kishan Kaul, supra 1 at pg 27.

by the AP Shah Committee should form the overarching framework for governing these rights and obligations.

For instance, data controllers should first and foremost be accountable for their collection, use and disclosure of personal data and be transparent about it. The rights of individuals such as choice and access should be respected by Data Controllers.

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?

Currently, specific technology solutions for auditing and managing data access permissions are being offered to enterprises for monitoring their data protection compliance requirements. These include:

1. ***Data discovery and flow mapping technologies***: Such technologies scan data repositories and resources to identify existing sensitive data, classify it appropriately in order to identify compliance issues, apply the appropriate security controls, or make decisions about storage optimization, deletion, archiving, legal holds, and other data governance matters.
2. ***Data access governance technologies***: These provide visibility into what and where sensitive data exists, and data access permissions and activities, and further allow enterprises to manage data access permissions and identify sensitive stale data. Such technologies are especially useful in automating these processes at scale thereby addressing challenges arising out of large data volumes.
3. ***Consent/data subject rights management solutions***: These help in managing consent of customers and employees, as well as enforcing their rights over the personal data that they share, allowing organizations to search, identify, segment, and amend personal data as necessary. These tools are especially useful in achieving transparency and enabling consumers' data access rights.

Evidently, specific technological capabilities already exist, which can be leveraged by individual enterprises that handle sensitive and personal data. Thus, the industry is capable of setting up a workforce of auditors which can undertake such monitoring. A potential effectuating mechanism is a cyber risk insurance framework, whereby frequent incidence of data breaches can be directly correlated to premiums that enterprises may be required to pay. Such a framework will also typically involve the participation of actuaries engaged by insurance providers for regular performance assessments of enterprises. Such frameworks are already being mulled over at the level of OECD, which has set up a project for assessing the market and nature of available insurance coverage, awareness of cyber risks and the role of insurance in risk measurement, mitigation and prevention; and the regulatory and policy issues relevant to the development of cyber insurance markets.[10]

An industry driven audit mechanism builds on accountability, and is a preferable alternative over a government set up technology architecture.

[10] http://www.oecd.org/daf/fin/insurance/OECD-Project-Cyber-Risk-Insurance.pdf

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?

Regulatory sandboxes help incubate new technology solutions whilst simultaneously informing regulators on good light touch regulatory practices, which encourage sustainable market growth.

Businesses should further be incentivised to share data relevant to their businesses so that other technology businesses can leverage the same to develop new products.

Ensure that ministries and departments regularly update pertinent information on open-source websites like data.gov.in which are designed to encourage research and innovation using government data.

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?

A data sandbox will allow for experimentation on data in a regulated manner. Such data sandboxes should however be set up after due consultation of stakeholders, to record the specific concerns and challenges faced by diverse industry members and users of the information.

Currently, a number of government data sandboxes have been set up across jurisdictions such as UK, US and Singapore, holding sector specific data – health, civic structure security, traffic management, and most notably, financial technology.

The Ministry of Communications and Information (MCI) of Singapore has sought to introduce a Data Sandbox Programme to facilitate data sharing and exchange. The programme aims to:

(i) Provide a neutral and trusted data exchange environment and analytics tools to help companies and government agencies experiment and discover the value of data and data exchange;

(ii) Conduct data discovery and analysis workshops to help level up companies' competencies and confidence in the use and exchange of data.

In order to carry this forward, their government is also setting up an API Exchange (APEX) in order to enable data sharing across domains and agencies, while also developing a Data Protection starter kit to help enable greater engagement of start-ups within the industry.[11]

A data sandbox requires appropriate regulatory allowances, along with clarity as to the scope for experimentation, as well as mechanisms to monitor and identify risks that may emerge from newly tested products.

The suggestion for setting up a government data sandbox is a welcome recommendation which incentivises innovation with available data. At the same time, datasets within the data sandboxes should be appropriately randomise/anonymised to ensure privacy of individual data.

[11] http://www.channelnewsasia.com/news/singapore/mci-unveils-digital-economy-strategy-for-people-firms-and-govern-8776964

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?

Privacy by Design is a relevant engineering principle that permits data processors and controllers to ensure privacy of information by protecting personal data through automated IT systems and practice that employ in-built privacy defaults. These include technical and organisational mechanisms that minimize data collection, collecting, retaining and using only data which required for the specific purpose and time period, after which it is securely destroyed. Additional measures like end-to-end encryption, user access to the data collected, and appropriate consent-obtaining mechanisms form part of this system.

The Information & Privacy Commissioner of Ontario, Canada has spearheaded the development of seven 'foundational principles of privacy by design', namely: (i) Proactive and preventive; (ii) Privacy as default; (iii) Embedded into design; (iv) Full functionality; (v) End-to-end security; (vi) Visibility and transparency; and (vii) Respect for user privacy (user-centric).[12] The UK Information Commissioner's Office takes these principles into account while recommending a privacy by design approach including a framework for Privacy Impact Assessments.[13] In the EU, the GDPR embeds the principle of privacy by design and default, wherein data controllers are required to implement appropriate technical and organisational measures for ensuring privacy, such as pseudonymisation and data minimization.[14] Moreover, the European Union Agency for Network and Information Security (ENISA) specifies technologies for implementing privacy by design for big data, with special focus on big data anonymization, encryption, privacy by security, transparency, access and control mechanisms.[15]

Privacy by design, by implementing important data protection measures through the embedded design itself, ensures consumer trust in their engagement with service providers, while enhancing overall security of the network infrastructure. It also creates an enabling environment for industry by minimising compliance risks and regulatory intervention and, at the same time, protects personal data from the get-go.

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?

Cyber-security is the shared responsibility of each member of the digital ecosystem where the government and the private sector leverage their respective strengths and compensate for their respective infirmities to create achieve ecosystem robustness. In this context, it is imperative to create an environment where stakeholders share pertinent incident or threat related information with one another. This is ensured through both formal means of coordination and informal means like WhatsApp groups. In this breath, certain critical elements for institutions like CERT-IN and National Critical Information Infrastructure Protection Centre (NCIIPC) must ensure both institutional

[12] https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf
[13] https://ico.org.uk/media/for-organisations/documents/1042196/trilateral-full-report.pdf
[14] http://www.eudataprotectionregulation.com/data-protection-design-by-default
[15] https://www.enisa.europa.eu/publications/big-data-protection

transparency as well as appropriate incentives such as proportionate reduction of penalties for enterprises to come forward with necessary information. At the same time, such information sharing should be done according to clear and precise rules so as to ensure consumer trust while disclosing personal information with relevant authorities.

In the specific context of telecommunication infrastructure, it is recommended that official standard setting institutions like the Telecommunications Engineering Centre (TEC) rely, as specified in the Unified Licensing Agreement, on standards developed by international standard setting bodies like ISO, IEC, IETF, IEEE etc. Moreover, to better reflect India's perspective (which is presently inadequately represented) in the realm of information and data security, the government should co-opt with key stakeholders to enhance India's participation at relevant international standard setting forums.

Additionally, technology-based safeguards such as cloud data protection through encryption of sensitive data before it goes to the cloud with the enterprise, helps address security, compliance and privacy concerns related to cloud based technologies. At the policy level, adoption of such technology solutions requires that appropriate encryption standards are not prohibited by the authorities.

Furthermore, possible policy measure mandating data localization must remain mindful of consequent trade-offs. For instance, it has been highlighted by organisations like the United States International Trade Commission that localization requirements can be problematic for cloud providers as it hampers location independence, which can lead to suboptimal storage of sensitive information.

Other best practice solutions such as tokenization and data classification help bolster ecosystem security and policy makers should incentivise their deployment.

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?

As discussed across this submission, we believe that data protection frameworks should be devised keeping in mind the following key issues:

1. Various emerging products and services employing machine-to-machine (M2M) applications and big data analytics require the exchange of information on a real-time basis. In this context, it becomes imperative that consent norms are developed to reflect the same.
2. Considering the global nature of data management and the internet in general, policymakers should aim to remain cognizant of the risks associated with restrictions on cross border flows on personal data. These risks include diminished flexibility for resource deployment for small businesses, which could inadvertently facilitate regulatory capture of large businesses over nascent technology sectors.
3. Emerging technologies, such as Artificial Intelligence, generally require access to data sets for development, thus, the new data protection regime should ensure that the development of such technologies is not unnecessarily hindered by onerous requirements.

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?

The proposed data protection law should typically govern the communications and digital sector under the same basic principles in a *technologically neutral* manner.

However, the respective roles of TSPs and other communication service providers like VOIP and messaging services are dissimilar and thus, parity between data protection norms between the two should be avoided. TSPs serve as the entry points for accessing the essential communication infrastructure, which in turn allows other communications service providers to run their applications. A technologically-neutral data protection law should adequately provide for harmonised data protection norms for TSPs and other communication service providers by recognising the nature of data being handled and the nature of processing activities being carried out. Under the Unified License, for instance, the TSP is responsible for maintain 'confidentiality of information' as well the security of the overall network. Such requirements have to be harmonised with the broader data protection laws such that externally sourced compliance requirements are not imposed on other providers of communication services. Once a common data protection law is enacted, the TRAI should review such provisions in the Indian Telegraph Act and licensing conditions to recommend appropriate changes that may be required.

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?

The Supreme Court has enumerated a three-fold requirement for intervention for the purposes of protecting legitimate state interests. These are –

(a) There must be a *law in existence* to justify an encroachment on privacy in conformity with the express requirement of Article 21.
(b) There should be a *legitimate state aim* to ensure that the nature and content of the law which imposes the restriction falls within the zone of reasonableness mandated by Article 14, which is a guarantee against arbitrary state action.
(c) The means which are adopted by the legislature are *proportional* to the object and needs sought to be fulfilled by the law.

The Court has also clarified that the government may gain access to personal information in an anonymised form for carrying out welfare functions. However, it is critical that such information is utilised in a non-discriminatory manner. Furthermore, the data controllers and internet content providers should be permitted to satisfy themselves with the fact that the request is legitimate since they are the custodians of user data. There should also be provisions in the data protection law which exempt the data controllers from liability for loss of customer data after it is handed over to the authorities in line with any of the exemptions under the law.

It should further be kept in mind that such exceptions should be restricted only for critical purposes such as national security or law enforcement and should conform to global best practices.

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?

The IT Act recognised the interconnected nature of data-based businesses and envisioned the same in its rules governing SPDI, allowing transfer of data across borders. Further, the IT Act (a statute passed in the year 2000) envisioned extra-territorial jurisdiction, extending to all offences governed by the Act.

Cross border data flows are essential not only for international trade and commerce, but serve as the very foundation on which essential services are provided to enterprises across the globe. The digital ecosystem consists of several services providers located around the world which provide the requisite infrastructure to newer enterprises in the form of cloud storage services and security services against Denial-of-Service (DOS) attacks, etc in a cost-effective and quality assured manner. These essential services engage servers located across jurisdictions, which necessitate simultaneous global data flows.

Restrictions on the cross-border transfer of data impedes access to such essential services, which are especially necessary for newer enterprises. Thus, such restrictions should be avoided. Data localization requirements, if any, should not be imposed solely on the ground of protectionism. Unreasonable restrictions on usage of data are prohibitive and counter-productive in providing India with simultaneous access to the world's best technology and products especially in the context of development of a cash-less and digital economy. Further, reciprocal restrictions by other jurisdictions can impede the growth of indigenously developed technology solutions if similar restrictions on Indian businesses are imposed.

In this context, jurisdictional challenges can be effectively addressed through strong mutual recognition and acceptance instruments with other jurisdictions. For instance, the United States – European Union privacy shield which grants 'deemed adequate' status to enterprises that have self-certified according to the stipulated privacy framework. Furthermore, multilateral agreements such as the Trans-Pacific Protocol also include provisions relating to cross-border data flows. In this light, jurisdictions which see high volumes of Indian data flows should be identified and engaged strategically and negotiated with.