NASSCOM-DSCI Submission to TRAI Consultation on Data Privacy in Telecom Sector

Preamble

NASSCOM & DSCI appreciate TRAI's endeavor of coming out with a consultation paper on the critical and germane area of Data Protection in the country and seeking inputs and comments from all the relevant stakeholders. NASSCOM & DSCI, by virtue of response to this consultation, reiterate and reaffirm the need for a balanced and calibrated approach for policy formulation with regard to Security, Privacy & ownership of Data. It is essential that this understanding echoes across the stakeholder groups and leads to better and enabling regulatory and policy ecosystem.

The current technological landscape and regulatory regime in the country is particularly interesting. The changing landscape warrants a regime which lends more clarity to the overall Data Economy, a state toward which India is moving precipitously, and also creates a conducive environment for businesses to flourish. Though, there is still lot of ground to be covered but the work has started especially with the data protection bill under making.

The proposed data protection bill in-making should not be over prescriptive while considering both socio as well as economic impact it may have on various businesses in India. We understand that the TRAI consultation paper would also serve as an input to this important activity. A summary of our suggestion are given below

- The need of the hour is to walk the fine balance between supporting and enabling global movement of data to facilitate commerce while, simultaneously, inspiring trust among individuals, industry and governments and enhancing their ability to control access to their data, even as economic value is generated out of such data collection and processing for all players.
- While the proposed data protection law will take care of basic privacy hygiene across sectors, nuanced provisions may be brought upon by sectoral regulators through subsequent guidelines/ rules. Therefore, while the Consultation Paper identifies various stakeholders in the entire data ecosystem such as device manufactures, content and application service providers, operating systems, browsers etc. that gather user Data, expectations and obligations of such players are very different from licensed Telecom Services and Internet service providers
    - Specific to licensed services by TSPs, TRAI could propose specific guidelines to preserve data privacy while providing licensed services.
    - TRAI can also facilitate development and adoption of a comprehensive data protection framework from the standpoint of telecom sector, while promoting efficient markets and the public interest.

Response to Questions

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?**

Prior to the recent Supreme Court verdict recognizing Privacy as a Fundamental Right guaranteed through constitution, the data protection space in India was regulated holistically by various sections and rules notified under Information Technology (Amendment) Act, 2008 and categorically and specifically by various sectoral regulators. The limited scope, enforcement, governance, understanding, accountability, etc. of the Act has always popped the requirement of a comprehensive privacy law in the country. Banks, Telecom Service provider, Healthcare and Insurance customers are custodians of personal information, and a data protection framework would serve to strengthen their practices and build customer confidence. Though, there is still lot of ground to be covered but the work has now started especially with the committee being constituted and tasked with formulating data protection bill. There is a need of no. of measures to be up taken by the government and regulator but many of the things would depend on how data protection bill comes into enactment. Some of the important aspects that needs attention can be:

- **Coverage**: Most of the Data Protection laws cover entire gamut of Personal Information (PI), while our existing laws do not cover it exhaustively. For e.g., IT Act is limited only to Computer and Computer Resources, and does not apply on physical form of data. It means that the law is applicable only when personal data is in electronic form and leaves the data available in hard copies such as medical records on paper, CAF forms by telecom operators, personal data collected on papers in various scenarios such as lucky draw at petrol pumps, etc.
- **Framework/Approach**: The regulation has addressed requirements of various privacy principles through rules notified in 2011 under section 43A, but has not listed them explicitly. The framework defining the privacy principles, their applicability and scope would be a standard approach.
- **Enforcement**: Unlike EU member states that have Data Protection Authorities or Information Commissioners or the USA where a nodal agency like Federal Trade Commission (FTC) oversees Privacy matters, and have the power to enforce privacy regulations, in India we do not have any such enforcement mechanism. Under ITAA, Adjudicating Officers are notified but they cannot take Suo-Moto action and can only order compensation to data subject, and not impose penalty or fines.
- **Unaddressed provisions**: There are various elements notified under the current regime, such as audit by government empaneled auditors, encryption requirements, data retention period, etc. which are not yet clearly defined in our laws. Hence, frequent reviews and guidelines on various aspects would be very crucial in upcoming data protection bill in India.

- **Technology Evolution:** Most of the countries, including EU continue to grapple with issue of how to contextually evolve Data Protection laws with changing technology landscape. IT Act provisions too could be termed as dated to address current challenges. Having a technology/platform neutral data protection law which applies horizontally across the ecosystem should be the path forward.

Data Protection regime of the country is currently not adequate due to lack of enforceable federal privacy law, but will expectedly be significantly strengthened once Data Protection law in enacted. Current regime is inadequate to protect the growing concerns of the telecom users with respect to the multiple types of Data being generated by telecom users – voice and video, call records, meta-Data, user generated contents of text, GPS Data/location services etc. The new law expectedly will set the baseline, and sectoral regulators like TRAI, RBI, IRDAI etc. might come up with sector specific privacy guidelines, if needed, arising out of sector specific characteristics. However, sector specific guidelines should not become means and ways to introduce stringent conditions negatively impacting citizens and/ or business competitiveness

It is a welcome effort that the Consultation Paper has attempted to identify various stakeholders in the entire data ecosystem such as device manufactures, content and application service providers, operating systems, browsers etc. that gather user Data. However, expectations and obligations of such players are very different from licensed Telecom Services provided by an organization for Telecom and Internet services. Hence once the data protection law is enacted, TRAI may review the existing provisions in the Indian Telegraph Act and licensing conditions (UAL) and issue advisories or guidelines for the licensed players for protecting personal information of users obtained under licensed services by telcos. Hence Telecom sector privacy specific guidelines should be specific to Telecom service providers (TSPs) for providing licensed services.

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?**

The definition of PI as defined under IT Act is limited to data available in IT systems of India, and electronic form of data (offline and paper records are not under the scope of current legislation). The horizon of PI is now broadening with evolving nature of businesses and technology innovation. A glance at the definitions of "Personal Data" in policies and legislations around the world reveal that it is often all inclusive and flexible.

Whether a particular piece of information is contextually a Personal Information capable of impacting privacy of an individual when breach, misused or shared is not easy to establish, and hence very difficult to forge a common ground concerning this especially under comprehensive federal data protection law.

EU Article 29 Working Party[i1] concluded that the test of whether information is personal or not is a dynamic one and should also consider the state of the art in technology at the time of the processing and the possibilities for development during the period for which Data will be processed.

Hence proposed legislation and/ or subsequent guidelines/ rules and case laws should try and recognize the role that purpose, context and proportionality play in determining whether a particular piece of information in isolation or in combination with other information constitutes personal information in that specific context, beyond the general rule. Contextual nature of data should be vitally considered, for e.g., anonymized data many a times can be considered as non-PI but one should note that the same data could be used to identify an individual in conjunction with the other data sets available publically. Hence, only defining the PI may not serve the purpose of overall data protection. Considering the digital nature of technologies generating large amount of data, out of which much can be constituted as PI if contextualized, could also be addressed by the sectoral regulators. As the regulation should strive to be technology neutral, the PI definition should be formulated keeping in mind various other aspects and nature of data such as purpose, collection, consent, access, proportionality with sensitivity, individual identifiability, etc.

There have been quite a no. of discussions on whether consent based privacy protection is enough or are there other mechanisms, but one should understand that taking consent is not the only thing but combining it with other factors helps.

Under EU GDPR Consent principle, consent should be informed, unambiguous, freely given, requires affirmative action (silence or non-action should not be deemed as consent), should not be mixed with T&C, must be demonstrable, revocable etc.

Organizations have been developing innovative ways such as one information piece-one consent, multiple consent, customized consent, customer friendly informed consent, action required consent, etc. while also operationalizing other privacy principles. The consent should not be considered as simply responsibility/liability transferring tool but should be practiced along with other privacy principles to provide desired respect to individuals' privacy.

The data protection regime in India too may identify the set of PI which requires explicit consent and other specific requirements but also consider the reasonability of executing it by the organizations.

Other factors which can define the meaning and serve the purpose of taking consent may be, but not limited to, sensitivity of data, time when it is taken, language used, notice provided, audience and repercussions of giving such consent. Various laws and regulations are being now amended/introduced to recommend/mandate the way consent is being taken by the data subjects.

The consent should not be considered as simply responsibility/liability transferring tool but should be practiced along with other privacy principles to provide desired respect to individuals' privacy

[1] EU Article 29 of Working Party - http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

User empowerment can cover various aspects which include efforts by government, regulator, organizations, educational institutes and others. Formulating and enacting a good legislation is only one part of effective regime, and proper enforcement, awareness and understanding of the same with individuals, government and organizations plays a very crucial role. Sensitization on the perils of a privacy breach for individuals/data subjects as well as organizations collecting and processing PI for business use is essential. Empowering users with privacy principles and adequate rights to control their personal data would be limited if users would not be aware of it or would not know the way of exercising the same. Globally, government and regulators not only mandate privacy principles and rights but also conduct awareness campaigns and obligate organizations to impart individuals with an understanding of how they may ay exercise their privacy rights.

In order to give better control over their personal data to individuals the following may be considered

- Access and rights to edit and rectify personal information - both information collected directly from individual, as well as developed by the organization basis monitoring the individual and has the potential to identify the individual in isolation.
- Data should be adequately anonymized and not include individuals' behavior, trend, digital/online profile, preferences, etc. which may breach individual's privacy.
- Data Controllers should be transparent on data usage and sharing, to provide users the confidence and build trust in the data ecosystem.
- Data Portability and Right to be Forgotten/Erasure are two specific rights that have been explicitly crafted in EU GDPR (European Union General Data Protection Regulation) for giving more control to the users over their personal data. With respect to the digitization story of India wherein several products and services are coming up, there is certainly an evolved expectation of Privacy of end users and citizens However, we should be mindful of the fact that such provisions if introduced shouldn't be onerous for businesses. But, user should be provided with appropriate tools and technology to meaningfully exercise their choices and preferences, with respect to processing of personal information.
- Other innovative ways maybe evaluated by the businesses to award more control to individuals over their personal data.

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.**

Rights are primarily granted by the constitution to the individuals and citizens, whose personal data is considered. Data controller will be subject to various responsibilities in order to exercise those rights and fulfill the individuals' demands, if any, while practicing their rights.

Currently, the data controller is not defined in any of the legislation or regulation in India. Body corporate, which is defined, also is limited to certain organizations and doesn't cover government organizations in general. There is a dire need of adequately defining the role of data controllers and data processors and corresponding obligations and practices that they should be observing while ensuring privacy of individuals.

The rights or duties or responsibilities of the data controller can be defined once the framework is designed as per the data protection bill in-making and would be guided by various privacy principles, governance structure, enforcement framework, rights to individuals, etc.

Sectoral recommendations/advisory/guidelines/requirements/framework can then further be developed in line to data protection bill and can suggest responsibilities of data controllers in order to enhance the overall privacy protection of consumers.

There is a dire need of adequately defining the role of data controllers and data processors and corresponding obligations and practices that they should be observing while ensuring privacy of individuals

There can be various obligations of data controller which may conflict with individuals' privacy such as retaining PI of individuals for specific time period even after consumer has asked to delete/erase, or disclosing the data to law enforcement agencies, etc. In such cases also, individuals should be informed about such activities/processing and ensure of limiting the data processing for specified purpose only. Such issues can be addressed largely by data protection law in-making and by sector specific regulation complementing the law for specific set of data and requirements.

To start with, the legal framework could recognize controllers to self-certify against misuse of data, against unauthorized sharing etc. to instill confidence in the users of the system. APEC (Asia Pacific Economic Cooperation) Privacy Framework which entails definition of PI, privacy principles, implementation guidelines, enforcement mechanisms, trans-border data flows, etc. may also be referred while defining data protection regime in India.

Various legislations across the world has designated data protection authorities at national level and have recommended data protection offices and officers at organization level, in order to craft both enforcement and governance framework.

We await the draft of the data protection bill for more details and can then make specific suggestions to the proposed framework.

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?**

There have been various initiatives at organizational level that started building resource capacity and capability both in terms of individuals as well as technology and processes. This was driven

majorly by the global requirements and contractual obligations on the IT-ITeS and BPM organizations while delivering various projects globally. Considering the rising privacy concern due to PI mass collection and usage by state and national projects, and increasing importance of privacy as a subject, International Centre for Information Systems and Audit (iCISA) of Comptroller and Auditor General of India (CAG) conducted training session on 'Data Privacy Audits of e-Governance Projects', in its auditors training program with an aim to build capacity on Privacy audits. Enforcement and governance framework supported with right approach (self-certification or self-declaration by the organizations, regulated by a data protection authority) would enhance the overall posture of India in terms of data protection and would enable businesses to benefit both directly and indirectly.

A co-regulatory framework (self-certification by organizations coupled with validation through third party audits) would go a long way in developing and maintaining audit governance and compliance.

DSCI frameworks & credentials

Since 2010, DSCI has come up with various initiatives and has developed significant capacity in the space. It developed, DSCI Privacy Framework (DPF©), to help organizations design, implement and monitor a comprehensive privacy program and demonstrate compliance. Adoption of the DPF© has been observed across various industry verticals amongst Indian organizations, especially in Banking and Telecom organizations. DSCI is also working with regulators like RBI and IRDAI in building a sound Privacy framework for organizations under their purview. Furthermore, in order to help organizations with their assessment of privacy program, DSCI developed an assessment framework (DAF-P) and for building the capacity around it, certification called DSCI Certified Privacy Lead Assessor (DCPLA©) and DSCI Certified Privacy Professional (DCPP©) were developed. DSCI also has its security framework and its assessment framework – DSF© and DAF-S. Through its training and certification programs, there are more than 500 privacy certified professionals from over 150 organizations across sectors, including government, banking, financial services, insurance, telecom and academia. There are also couple of organizations that have undergone assessment by DSCI's authorized partner Assessment Organizations (AOs) for attaining DSCI Privacy Certified (DPC©) organization status, while many are undergoing preparation to get their practices assessed and certified.

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 data protection framework should be enacted with regulatory certainty, consistency and appropriate guidance for the data controllers and processors in India, and should not act as trade inhibitor.

It should not be over prescriptive while considering both socio as well as economic impact it may have on various businesses in India.

There are no. of Internet-enabled services and apps and data driven innovation in India shaping up the digital India, which should not be negatively impacted by over prescriptive data protection bill in India.

The framework should recognize the already available solutions along with encouraging the innovation in the field of data protection. Innovative products and services in privacy space can be encouraged which not only serve the purpose of helping organizations comply with regulations but also prove to be economical viz-a-viz helping businesses establish trust and transparency to customers.

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?**

   Given the status of data rich economy India is en route to acquiring, it is imperative to seriously start considering a robust and forward looking open data policy. Data is extremely important for developing new products. Emerging companies, start-ups can hugely benefit from access to data.

   A regulatory data sandbox, different from a technology data sandbox, serves the purpose of facilitating thriving environment for innovative ideas with regard to the regulatory landscape.

   Regulatory data sandbox may be set up by the authorized authority with due regard to the fact that this sandbox is technology neutral and in no way restrictive of technology. Also, the government or the authorized authority should ensure that the clarifications sought by companies regarding regulations should be addressed in a time-bound fashion. And lastly, the conditions of industry reporting and disclosure shouldn't be onerous in nature.

   Setting up a data sandbox is only one such technique which may help organizations test and develop new services for customers, instead there should be a framework which encourage organizations to develop services without impacting privacy of individuals. Organizations restricting themselves while collecting limited PI for only desired and legitimate purpose, and following reasonable security and privacy measures, while developing and delivering services may help them comply with data protection bill on one hand and grow business on the other. Data sandboxing, sample data to play with, restricting use of data and many others can be technical and governance measures that can be practiced and not necessarily by the government but also by the industry and various institutes, incubation centers, etc. Sandboxing, though a good idea, shouldn't be mandated for organizations.

   It is important that the data collected, generated and processed by the government and businesses should be adequately protected. Big Data Analytics, which involves examining large Data sets to uncover hidden patterns, unknown correlations, market trends and other useful information, require that balance be maintained on data protection and anonymized data usage. Like the government has established Open Data policy, some mechanism for private sector players to also share completely anonymized data for general analytics and innovations should be established. It will result in more data based innovation, without necessarily compromising Privacy.

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?**

Technology developments are very dynamic and attempts to monitor for compliance will likely place significant, if not overwhelming, burden to operate such a system. Additionally it might raise privacy concerns as an unintended outcome. There is a need for more efficient solutions in monitoring, compliance and governance space.

In this regard solutions with suitable capabilities and effectiveness need to be explored as part of a more concerted approach towards ensuring compliance in the ecosystem. There is always room for improvement as advanced technologies are being developed and adopted across industries.

To bring more accountability to the organization, self-regulation should be promoted along with enforcing the end user through adequate grievance redressal mechanism. Self-certification or self-declaration present a more constructive approach and could be promoted as a way to go when it comes to compliance and enforcement. Please refer the response for fourth question for elaboration of this point.

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?

A vicious cyber-attack on a telecommunications operator could potentially disrupt service for millions of customers cripple businesses, and bring government operations and services to a halt. Today's cyber adversaries are constantly sharpening and evolving their capabilities to exploit new vulnerabilities. Addressing these threats will require that telecoms operators approach activities and investments with comprehensive, up-to-the-minute knowledge about information assets, ecosystem threats, and vulnerabilities.

In order to safeguard the integrity and security of a standards-based telecommunications infrastructure, departments must implement baseline security controls and any additional security measures identified through a Threat and Risk Assessment process. Once again, a holistic and pragmatic approach must be followed taking into account the sensitivity of the information being processed. Because it is costly and time consuming to re-arrange physical barriers in response to changes in tenancy of a space, other measures must be considered to ensure that proper balance is maintained between the potential threats and the safeguards.

In addition to physical security, departments must take into account operational and technological considerations as well. Solutions such as strong encryption help meet their overall security goal. Current safeguards under IT Act and other legislations may not suffice from a perspective of protecting critical infra protection. There is a need for close coordination among the Cyber Security agencies for better response to incidents and of course robust preparedness and adherence to best practices can't be emphasized enough. Forging public private partnerships ``````````to thwart such attempts is another measure that needs to be encouraged.

Capacity building is another critical aspect when it comes to safeguarding the infrastructure from vicious attacks. This includes hiring the right experts and continuous upgradation of the talent to keep up with the threat landscape. Both Industry and the government should work in tandem to generate a pool of Cyber Security specialists

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?**

All data controllers should be responsible for protecting the privacy of their users under the proposed data protection law 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. Obligations of other stakeholders including the data processors could be governed by the legal contracts.

Key issues pertaining to collection and use of data

- failure to have the appropriate legal authority to collect, use or disclose personal information;
- excessive collection of PII (loss of operational control);
- unauthorized access to PII (loss of confidentiality);
- unauthorized modification of the PII (loss of integrity);
- loss, theft or unauthorized removal of the PII (loss of availability);
- unauthorized or inappropriate linking of PII;
- failure to keep information appropriately secure;
- retention of personal information for longer than necessary;
- processing of PII without the knowledge or consent of the PII principal (unless such processing is provided for in the relevant legislation or regulation); and
- sharing or repurposing PII with third parties without the explicit informed consent of the data subject

Mechanisms to address the issues

- User shall be provided detail scope where his data would be used for.
- Self-certification on privacy policy and practices
- Explicit and unambiguous consent from the users for PII and sensitive data sets
- Notifications to the users in case of any changes
- Provision of a single dashboard on devices, platforms, systems, apps etc. to provide end to end visibility on privacy settings and on its control

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?**

There is a strong feeling that the Data protection rules or norms or standards that are being framed currently under the aegis of the Data protection committee must be technology and platform agnostic. These should be mandated equally for each Data controller and reasonably for data processor (through contractual means) across domain to control the breach and misuse of PII/SPI.

From the telecom sector standpoint, since the telegraph act and the DOT licensing conditions currently address the issue of Data protection, once the Data protection framework is in place, these would merit a relook from the concerned authorities to bring them in line with the proposed legislation.

In the interest of clarity and simplicity, differentiation should be made between '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 be 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.

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?

As TSPs functionality have multiple layered dependency on several vendors as MSPs, Payment Gateway, Billing, VAS, Packet Core, etc. so data controllers shall ensure the Privacy policy is adhered by all connected vendors and sub vendors. While adhering to policy, the processes to be followed by data processors should be clearly defined in the contracts by the data controller which may also not put unreasonable liabilities on to data processors.

With regard to lawful interception, distinction should be made between controller and processor role of TSPs and the LEAs should keep in mind the role of the organization while seeking access to information. The lawful surveillance and law enforcements requirements as per IT Act is open ended with no clear exceptions defined. The future data protection law should clearly call out situations of public emergencies or national security with indicative examples for enhanced clarification. For e.g., LEAs should be asking for legitimate and specific data points helpful in investigating a crime and hence demand for generic data dump should be avoided. Legitimate exception should only be on legal grounds.

The data protection law should have judicial interventions and oversight for surveillance and lawful access to data. Also, the legal regime should enhance privacy safeguards based on sensitivity of the data being accessed/intercepted

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?

A. **<u>Cross Border Data Flow and Data Localization</u>**:

Cross border data flows are fundamental to a majority business models and should not be heavily regulated; doing so can impact the digital economy severely. Today data flows and its use is as much important to large MNCS as is to businesses who may not be in the high tech sector and consumers.

The regulatory requirements and current regime differs from country to country, in case of trans-border data flows and disclosure requirements. Compliance with data protection regulations, that seem to be becoming more stringent in different parts of the world, especially in European countries, is posing increased challenges to the free flow of information across borders and is impacting the IT/BPO industry in India.

Countries are increasingly becoming concerned about free data flows for a variety of reasons such as

- revelations about the ability of governments to collect digital traffic;
- protectionist goals to favor local companies;
- concerns about the security of personal data of its citizens to just name a few.

Drastic, yet a common policy response to the problem that is seemingly getting traction is the mandatory requirement on storing critical data on servers physically located inside the country. Barriers are being imposed on the free flow of data across borders by various nations, both developed and developing. While many of these issues and concerns need global discussions and solutions, the knee-jerk reaction of governments which favours data localization / regulation of content providers is a matter of great concern. **Subjecting organizations to the requirements of data/infrastructure localization will prove to be counterproductive** for variety of reasons including:

- Localization requirements prohibits organizations from achieving economies of scale and leveraging global souring hyperspecialization benefits, resulting in increasing cost of services that could be passed on to consumers
- Localization adversely affects exports and may deter organizations from undertaking cross border businesses
- It may threaten major new advances in technology and innovation
- It threatens open architecture of the Internet
- If similar policy directions are followed by other countries, it will severely hit established Indian IT-BPM industry sector including the emerging cloud industry which is major contributor to the Indian GDP

Barriers to free data flows form considerable obstacles to global trade. Customers would find

themselves unable to access valuable digital services. Small and medium-sized enterprises (SMEs), which could greatly benefit from digital trade, would be disproportionately affected by these barriers. They do not have the resources to bear these unnecessary costs, and are far more restricted in their global reach.

Data is an essential resource for healthy economic growth and that excessive restrictions on data will be a barrier to secure management and protection of data. A principled policy approach which recognizes that data regulations must be simple, transparent and harmonized with other legislative requirements. Forced localization of data requirements interrupt the free flow of data that underpins the complex online networks connecting the globe in ways that threaten the cultural and economic growth potential of the Internet and Internet-based technologies. India should develop and propose policies that help leverage international arrangements on cross border data flows, as it benefits its outsourcing industry competence.

B. Issue of jurisdiction is also an important issue from the viewpoint of applicable laws and regulation. The location of storage and processing of data determines what laws will apply. To overcome the challenges of Extra-terrestrial access to data by LEAs, governments including **India should work with the other nations in plurilateral, multilateral and bilateral forums to discuss and come out with practical solutions.** In the age of Internet, global cooperation is quintessential and therefore India should take leadership in identified forums to ensure that its issues are addressed. For example, India should pace up the dialogue on Mutual Legal Assistance Treaty (MLAT) reforms with the U.S. or negotiate a special process for speedy data sharing on crime investigations with the U.S. as presently the Indian LEAs face issues when getting access to data records required from datacenters in the U.S. for investigating crimes that happened in India. India has signed a Cyber Fact Sheet with US, and timely access to information and cooperation amongst LEAs is an important consideration in the dialogue between the two nations. Similarly, US Department of Justice is trying to amend its practices so that LEAs of other nation states, can directly get access to data from Organizations established and storing data in the US. US and UK are also deliberating on an alternative for MLAT between them. India should try and work out such a mechanism with US and other nation states as well. India should strengthen bilateral, multilaterals, plurilaterals, international treaties and other such mechanisms, and look to improve existing procedures for quick and effective information sharing and getting lawful access to data. **India should reconsider and revaluate Budapest conventions pros and cons, and whether it should result in something meaningful. If India were to become signatory to it.**

Also, Indian LEAs should also be effectively resourced and trained to raise legal requests for gaining lawful access to data from CSPs not located in India through the MLAT route. Further, there is also a dire need to improve procedures and frameworks for data sought by LEAs from CSPs both in India and abroad. Regarding Lawful interception for data hosted outside India, if it is not done with knowledge of country where data is hosted, it might amount to Surveillance/ Espionage. Hence due legal processes, with precise interpretation of international laws, should be followed by LEAs for obtaining data hosted outside territorial jurisdiction of India.

In order to effectively address some of the aforementioned issues, we could begin by adopting some of the following measures:

- APEC CBPR(Cross-border Privacy rules) could serve as a good model while formulating trans-border data protection requirements as part of India's Data Protection regime
- Discuss and deliberate different approaches / recommendations that can help Indian outsourcing industry overcome the identified challenges. For e.g. harmonization of regulatory requirements, lobbying with regulatory bodies to categorize India as a country having 'adequate level of protection', 'Binding Safe Processor Rules' for data processors like 'Binding Corporate Rules' for MNCs etc.
- Identify partners for submitting and discussing the identified issues and approaches / recommendations. For e.g. WTO, WITSA, EU, DPAs, FTC, etc.

[i] EU Article 29 of Working Party - http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083