Collaborating for Competitiveness

No.:133/TRAI/2017-18/ACTO

Dated: 6th November, 2017

Shri Arvind Kumar
Advisor (BB&PA)
Telecom Regulatory Authority of India
Mahanagar Door Sanchar Bhawan,
Jawahar Lal Nehru Marg,
New Delhi-110002

Subject: ACTO's response to TRAI Consultation Paper No. 09/2017 dated 9th August 2017 on Privacy, Security and Ownership of the Data in the Telecom Sector

Dear Sir,

Association of Competitive Telecom Operators (ACTO) is pleased to submit its response to TRAI Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector.

We hope that our comments (enclosed as Annexure - I) will merit consideration of the Hon'ble Authority.

Thanking you,
Respectfully submitted

Yours sincerely,
for **Association of Competitive Telecom Operators**

Tapan K. Patra
Director

Encl: As above

ANNEXURE-I

ACTO's response to TRAI CP on Privacy, Security and Ownership of the Data in the Telecom Sector

(Consultation Paper No. 09/2016, August 9, 2017)

Introduction and Summary

ACTO respectfully submits these comments on the TRAI Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector, issued on August 9, 2017. ACTO also appreciates the opportunity to express its views in this consultation and hopes that its responses will be helpful to the Authority in formulating the recommendation keeping the right balance between data privacy and required business needs.

Over the last decades, Information and Communications Technologies (ICTs), including the Internet, have become essential to the functioning of the economy as well as a key driver for development in all sectors. Governments, public and private organisations as well as individuals have become dependent on the digital environment for their activities. However, they are facing a growing number of uncertainties related to the use of the digital environment as digital security threats and incidents have increased, leading to significant financial, privacy, and reputational consequences, and in some cases even to physical damages. Although stakeholders are increasingly aware of the challenges raised by digital security risk, they often approach it only from the technical perspective, and in a manner isolated from economic and social decision making. It should be integral to economic and social decision making in order to enable stakeholders to fully benefit from the opportunities offered by the digital environment.

ACTO Members are committed to protect the privacy and security of their enterprise customers' data. We recognize that establishing a trusted environment for businesses, consumers across the digital ecosystem is crucial to the success of the market.

The framework for privacy regulation must be technologically neutral and interoperable with international standards. Specifically, the Privacy Act should not make any reference to specific technologies and must be generic enough such that the principles and enforcement mechanisms remain adaptable to changes in society, the marketplace, technology, and the government. To do this it is important to ensure the consistency of the right to privacy with

multiple international regimes, create trust and facilitate co-operation between national and international stakeholders and provide equal and adequate levels of protection to data processed inside India as well as outside it. In doing so, the framework should recognise that data has economic value, and that global data flows generate value for the individual as data creator, and for businesses that collect and process such data. Thus, one of the focuses of the framework should be on inspiring the trust of global clients and their end users, without compromising the interests of domestic customers in enhancing their privacy protection.

It should be from best practices internationally, such as Asia Pacific Economic Co-operation (APEC) and Organisation for Economic Co-operation and Development (OECD) Privacy Frameworks, adapted suitably to an India context, that the baseline level of privacy protection to all individual data subjects is drafted. The fundamental philosophy underlining the principles is the need to hold the data controller accountable for the collection, processing and use to which the data is put thereby ensuring that the privacy of the data subject is guaranteed.

As we provide our comments to the questions raised in the paper, we submit that the privacy recommendations should be based on the following key principles:

a) **Privacy rules to be uniform across the entire ecosystem**.

In a connected world where individuals use multiple devices and services from different providers, privacy regulations that apply to only one set of technologies, data class or industry players can create customer confusion: consumers expect that one set of rules will apply to the processing of their personal data, regardless of whether a device manufacturer, an application provider, or a connectivity provider does the processing. Promoting consistency helps mitigate this confusion and satisfy customer expectations.

b) **Privacy rules to be based on the sensitivity of the information collected and used**.

Rules and protections should be tailored to context and strike the balance of targeting potentially harmful uses of consumer data while allowing its many beneficial uses.

c) **New and Emerging technologies the Internet of Things (IoT) do not require the invention of new regulations for privacy and security**.

Privacy in the IoT requires a balance of traditional standards and new methods: principles such as data minimization remain relevant, but they should be flexible to allow for innovation and development of future consumer and societal benefits of collecting and using such data.

d) Cross-border data transfer mechanisms are essential to the global digital economy, and governments should ensure that these are predictable and interoperable.

Governments can build trust in the global economy – and specifically in the cloud computing and IoT industries – by creating an environment for service providers to follow industry best practices and guidelines regarding the cross-border use and protection of personal data, while providing appropriate accountability mechanisms for those who wish to challenge data management practices. Agreements such as the APEC Cross-Border Privacy Rules Framework, Privacy Shield, and the EU-US Principles for ICT Services should be considered.

ACTO's response to the specific questions raised in the consultation paper:

Q.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?

ACTO's response:

ACTO members believe that data privacy rules should be consistent across the digital ecosystem. In a connected world where individuals use multiple devices and services from different providers, privacy regulations that apply to only one set of technologies, data class or industry players can create customer confusion: consumers expect that one set of rules will apply to the processing of their personal data, regardless of whether a device manufacturer, an application provider, or a connectivity provider does the processing. Promoting consistency helps mitigate this confusion and satisfy customer expectations.

Privacy rules should be based on the sensitivity of the information collected and used. Rules and protections should be tailored to context and strike the balance of targeting potentially harmful uses of consumer data while allowing its many beneficial uses.

The data protection requirements to protect the interests of telecom subscribers are sufficiently captured under the provisions of the Telecom License Agreement as well. Additionally the collection, storage and use of personal data in India is primarily governed by the provisions contained in the Information Technology Act 2000(IT Act). In particular Section 43A of the IT Act provides for compensation in the event that a company fails to use reasonable security practices and procedures in order to protect sensitive personal data and such negligence results in a wrongful gain or loss.

In addition to this there are sector specific vertical regulations that are imposed on the service providers as an additional Data protection requirement such as the Financial Services, banking, Telecoms and Healthcare Sector. Specific for Telecom Subscribers, there are suitable provisions incorporated in the Licenses issued to the Telecom Service providers.

The current Data Protection requirement applicable to Telecom providers as per the ILD License agreement are reproduced below:

21. CONFIDENTIALITY OF INFORMATION

21.2 Subject to conditions contained in these terms & conditions, the LICENSEE shall take all necessary steps to safeguard the privacy and confidentiality of any information about a third party and its business to whom it provides the SERVICE and from whom it has acquired such information by virtue of the SERVICE and shall use its best endeavours to secure that:

a) No person acting on behalf of the LICENSEE or any member of the LICENSEE's group (associates) divulges or uses any such information except as may be necessary in the course of providing such SERVICE to the Third Party; and

b) No such person seeks such information other than is necessary for the purpose of providing SERVICE to the Third Party.

<u>Provided the above para shall not apply where:</u>

a) The information relates to a specific party and that party has consented in writing to such information being divulged or used, and such information is divulged or used in accordance with the terms of that consent; or

b) The information is already open to the public and otherwise known.

21.3 The LICENSEE shall take necessary steps to ensure that the LICENSEE and any person(s) acting on its behalf and members of the LICENSEE's group (associates) and any persons acting on their behalf observe confidentiality of customer information.

21.4 The LICENSEE shall, prior to commencement of SERVICE, confirm in writing to the LICENSOR that the LICENSEE has taken all necessary steps to ensure that it and its employees are observing confidentiality of customer information.

The existing provisions under the telecom licenses aptly cover the privacy requirements and there is no requirement for any addition as it binds the licensee. For example the following clauses of the internet service license clearly state the privacy and data protection requirements which a licensed ISP has to adhere with few stated exceptions: These are sufficient and have been mandated ever since licenses were issued.

32.1 However, the LICENSEE shall have the responsibility to ensure protection of privacy of communication and to ensure that un-authorised interception of MESSAGE does not take place.

32.2 Subject to conditions contained in these terms and conditions, the LICENSEE shall take all necessary steps to safeguard the privacy and confidentiality of any information about a third party and its business to whom it provides the SERVICE and from whom it has acquired such information by virtue of the SERVICE provided and shall use its best endeavors to secure that:

(i) No person acting on behalf of the LICENSEE or the LICENSEE divulges or uses any such information except as may be necessary in the course of providing such SERVICE to the Third Party; and

(ii) No such person seeks such information other than is necessary for the purpose of providing SERVICE to the Third Party.

Provided the above para shall not apply where:

(i) The information relates to a specific party and that party has consented in writing to such information being divulged or used, and such information is divulged or used in accordance with the terms of that consent;

or

(ii) The information is already open to the public and otherwise known.

32.3 The LICENSEE shall take necessary steps to ensure that the LICENSEE and any person(s) acting on its behalf observe confidentiality of customer information.

32.4 The LICENSEE shall, prior to commencement of SERVICE, confirm in writing to the LICENSOR that the LICENSEE has taken all necessary steps to ensure that it and its employees shall observe confidentiality of customer information.

34.10 The LICENSEE shall be responsible for ensuring privacy of communication on its network and also to ensure that unauthorized interception of message does not take place.

In view of the above, we feel that there is no need for introduction of additional sector specific measures in view of robust measures currently in place via License requirements and Information Technology Act. Additional measures can be considered only where it is necessary and proportionate. Additional measures, if any should only be considered based on any evidence of harm to the sector that to with prior industry consultation.

Q. 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?

ACTO's response:

Privacy frameworks in the United States and Europe provide individuals with different levels of control over the collection and use of their information depending on its sensitivity. Individuals are generally permitted to opt out of the collection and use of their personal information for purposes that are distinct from the original purpose of collection. Individuals can also generally restrict a company from sharing their personal information with non-affiliated third parties. Companies are permitted to use personal information to engage in first-party marketing to customers. However, collection and use of sensitive personal information requires an individual's opt-in consent under both the U.S. Federal Trade Commission's privacy framework and the EU General Data Protection Regulation.

Businesses should engage in efforts to educate and raise awareness of privacy risks and ways to mitigate them. By emphasizing transparency and individual consent, the current privacy framework imposes significant, sometimes unrealistic obligations on both businesses and individuals. On the one hand, businesses are expected to explain their data processing activities on increasingly small screens and seek consent from often-uninterested individuals; on the other hand, individuals are expected to understand complicated privacy disclosures and knowingly consent to them. The data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

a. In India, the definition of personal data ("personal information") is contained in IT Act 2000 rule 2(1)(h) of the Personal Data Rules as data which directly identifies a person or can be connected with other data to indirectly identify a person.

b. The Indian definition of personal data is in line with international norms. The direct/indirect dual classification of personal data is found in the laws of the United States, most European countries, Australia, Singapore, Japan, and others.

The definition of personal data should avoid being too broad & ambiguous, framing almost all general information as personal data. The definition of personal data should not include information that has no immediate connection to a specific individual. Any new data protection framework should allow for the use of de-identified data and aggregate data.

Consent

With regards to consent, we suggest TRAI to refer Singapore's Review of Personal Data Protection Act in Indian Context.

"Notification of purpose" requirement has been proposed by the Singapore Personal Data Protection Commission as per the Public Consultation for Approaches for Managing Personal Data in the Digital Economy issued on 27th July 2017. The paper seeks to replace consent where it is not practically possible to seek user consent before sharing his/her personal data for commercial purposes. In these situations, it is good practice to provide individuals with the capacity to opt out of data collection or to contact the organization collecting the data, where feasible . Such challenges for a consent regime may be present in the context of Smart Cities, the use of unmanned aerial vehicles or in retail centers that employ Wifi hotspots. As the paper notes the fast emerging Digital Economy is presenting challenges for consent based approaches to personal data protection. The growth of IOT devices, machine learning, Artificial Intelligence has given rise to the ability to collate and analyze large amounts of data, opening up new possibilities to derive insights that can yield enormous benefits for individuals and society. Thus relying only on consent for the collection, use and disclosure of personal data may have deleterious effects. An approach that calibrates the balance of responsibilities and adopt pre emptive preventive measures can meaningfully address the consent requirements.

With the above in mind, data privacy continues to be a rapidly developing area on a global scale. Any policy in India should follow a legal framework that relies on strong principles and business-level accountability to avoid over-expansive and inflexible regulations.

Q.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.

ACTO's response:

Data should be collected only for a specific stated purpose. Data once collected must only be used for the purpose for which it was collected. If a data controller is allowed to indiscriminately use the data collected, it would vitiate the informed consent obtained prior to collection. If personal data is to be re-used for a different purpose the data subject should generally be informed and provided with a measure of control prior to such use. Implicit in this provision is the obligation on the data controller to only collect that amount of data as is necessary for the stated purpose and no more.

Accountability is a principle reflected in the APEC and OECD Privacy Frameworks, and businesses should take proactive measures to implement concepts like privacy by design and data breach notification, consistent with this principle. Authorities should undertake analysis of the economics of remedies and sanctions by enforcement authorities, as well as trying to enhance international regulatory cooperation and interoperability of regulatory frameworks.

Some countries that have adopted data protection legislations have established a special regulator to deal with contraventions of the legislation as well as to more proactively supervise compliance with the statute. It can be light handed regulation through office of Ombudsman and reliance on self regulation by government and industry bodies. It is particularly important to develop the concept of accountability so that it should no longer be sufficient for organisations to meet applicable data protection requirements – they should demonstrate their willingness and ability to take on data responsibility and ensure compliance on an ongoing basis.

New technologies such as Big Data and the Internet of Things (IoT) do not require the invention of new regulations for privacy and security. Privacy in the IoT requires a balance of traditional standards and new methods: principles such as data minimization remain relevant, but they

should be flexible to allow for innovation and development of future consumer and societal benefits of collecting and using such data.

In light of the tremendous potential of IoT technologies and Big Data analytics, limitations on uses of data in these contexts should be qualified and proportional to the risk of privacy harm that consumers might suffer if their data is misused. Valuable insights can be gained from data when responsible companies use proper safeguards. De-identification and pseudonymization of data are effective practices for addressing privacy risk and should be encouraged.

Q. 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?

ACTO's response:

Rather than investing resources in an audit mechanism, the focus should be on enforcement of existing rules, targeting uses of data that create a risk of harm to individuals. Industry voluntary efforts, best practice codes and multi-stakeholder initiatives all drive privacy protections in ways that make sense for the providers and consumers of covered technologies, particularly when these are accompanied by accountability mechanisms.

Q. 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?

ACTO's response:

Governments can build trust in the global economy – and specifically in the cloud computing and IoT industries – by creating an environment for service providers to follow industry best practices and guidelines regarding the use and protection of personal data, while providing appropriate accountability mechanisms for those who wish to challenge data management practices. A light touch policy framework should be based on general standards and not be prescriptive in nature. Otherwise, regulation will not keep pace with rapidly evolving technology and markets.

It is important to highlight that in order for the creation of new data based businesses consistent with the overall framework of data protection, we would suggest that TRAI explicitly recognize a

distinction between data based residential services (sold to consumers) and data based non-residential services (sold to (large) business customers) to avoid automatically extending consumer protection obligations to the enterprise providers.

Secondly not all providers have a direct relationship with the individuals that are using the communications service in question. Some providers do not offer services directly to individuals. For example they offer services at the wholesale level or to enterprises and are therefore at least one step removed from the individual end user. For this reason they may not only have difficulty in determining whether a specific incident may impact personal data, but may also not have the capability to identify individuals affected by an incident. In such cases, providers should only notify their customers (subscribers) who have the ability to notify the individual of any potential personal data breach within their reach.

Q.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?

ACTO's response:

If the Government were to establish such a tool, industry participation should be voluntary and industry should not be compelled to surrender proprietary data. The Government should also take note of industry-led data-sharing platforms that are currently under development and seek to learn from, participate in, and encourage the development of best practices related to these efforts. To the extent such a tool is established, strong encryption and other safeguards will be essential.

Q. 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?

ACTO's response:

ACTO members recognize that governments can have a legitimate interest in addressing important objectives such as national security, public safety, law enforcement, and preventing harm to children. We also believe that government legal regimes should respond to technological changes through fair, accountable and uniform procedures that govern when and how private companies may be compelled by the government to provide information.

Q. 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?

ACTO's response:

ICT sector, touches nearly everything and everyone, and, along with energy, forms a foundation upon which all other critical infrastructure operates. A successful cyber attack on a telecommunications operator could disrupt service for thousands of home customers, sever Internet service for millions of consumers, cripple businesses, and shut down government operations. Telecoms operators are adept at protecting their networks. It's also true that cyber adversaries employ the telecom infrastructure as their primary transport for most attacks – and, as such, they rely upon a robust network.

Core practices like employee awareness and training, policies and tools to reduce insider risks, and protection of data – including intellectual property – will need to be updated.

Technology safeguards, of course, are another foundational element to secure telecoms ecosystems against today's evolving threats. Operators are deploying solutions that augment threat detection and intelligence capabilities. It is noticed that operator's increase use of technology safeguards like intrusion-detection tools, asset-management tools, protection and detection solutions, patch-management tools, centralized user data storage, and more.

Today, information security is a discipline that demands advanced technologies and processes, a skill set based on counterintelligence techniques, and the unwavering support of top executives. As telecom operators become more similar to technology companies, they will face a raft of new challenges.

Another new approach is sharing information with others to improve security and gain intelligence on current threats.

- One of the measures that can be considered in order to strengthen an preserve the safety and security of telecom infrastructure and digital ecosystem as a whole is to release the much needed strong encryption policy. The primary means of achieving this is to promote widespread use of strong encryption. However, industry is still waiting for the rules to govern encryption under section 84A of the IT Act to promote strong encryption.

- The telecom licenses should be suitably amended to remove the archaic limits on the use of encryption requirements where Indian ISPs are bound to 40-bit encryption keys limits.

- The government should encourage the use of end-to-end encryption wherever possible. Encryption regulations should be harmonised to unanimously promote the use of strong encryption. The government should issue rules under the IT Act to compel the use of strong encryption.

  The draft encryption policy issued by the MeiTy last year was a step in right direction to ensure the safety and security of telecommunications infrastructure and the digital ecosystem as a whole; we would encourage government to issue the encryption policy as envisaged under section 84 of the IT Act.

Q. 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?

ACTO's response:

One of the key issues is absence of distinction between sensitive and regular personal data. Sensitive personal data must be treated differently from regular personal data. At present no legislation makes this distinction. Data protection provision should create these categories to ensure that some forms of personal data are treated more specially than others.

Q. 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?

ACTO's response:

The Data protection norms should be horizontal rather than sector specific to reflect market dynamics and recognition of need for a flexible, technology neutral, and future proof Data privacy framework. The DP framework should aim to promote a lighter touch horizontal regulatory regime for all market players including internet based voice and messaging services to encourage investment and innovation in these new types of services. Therefore there is no

need for introduction of additional Data Protection requirements to bring parity as the Data Protection requirements as incorporated in the IT act applies to all the stakeholders in the internet ecosystem. Further the Data Protection law needs to flexible to enable & support new age digital services which can flourish only when international cross border data flows are enabled. We need to keep our approach to data protection dynamic so that we can remain nimble and responsive to a constantly changing privacy environment.

Q. 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?

ACTO's response:

All data protection legislations/regulations have in-built exceptions that limit the applicability of the legislation in the context of certain statutorily established circumstances. These could include national security interests, statutory functions, disclosures required by law or as part of legal proceedings, etc. There could be several specific exemptions that are particular to the Indian social and economic environment.

In the Indian context, the articulation of legitimate exceptions must be carefully defined to ensure that the purpose for framing of the legislation is not diluted so much as to make it meaningless. Thus, while national security exemptions are necessary and legitimate, they should be framed carefully to ensure that it is not possible for just anyone to claim that the provisions of the law are not applicable by citing some national security interest without substantiation

In order to provide legal certainty and guarantee privacy as effectively as possible, such exemptions should be based on minimum principles and safeguards of due process that national legislations on law enforcement access to data should respect such as being based on law, limited to what is strictly necessary for the investigation in question; focus on data of individuals impacted in the crime; be reasoned and subject to review and decision by a court or an independent authorities. The persons who can claim the exemption and the circumstances should be carefully limited.

The scope of bilateral and multilateral agreements may be enhanced for sharing information based on principles of transparency and accountability. Finding a balance is important if the full benefits of international trade in goods, services and e-commerce are to be realized by reducing unnecessary costs of doing business. Transparent and efficient mechanisms based on the rule of law are critical to building trust between countries in this area.

Q.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?

ACTO's response:

Cross-border data transfer mechanisms are essential to the global digital economy, and governments should ensure that these are predictable and interoperable. Governments can build trust in the global economy – and specifically in the cloud computing and IoT industries – by creating an environment for service providers to follow industry best practices and guidelines regarding the cross-border use and protection of personal data, while providing appropriate accountability mechanisms for those who wish to challenge data management practices. Agreements such as the APEC Cross-Border Privacy Rules Framework, Privacy Shield, and the EU-US Principles for ICT Services are positive examples.

Governments should commit to using Mutual Legal Assistance Treaties (MLAT) and processes when they seek access to data that is stored beyond their borders. ACTO members support government efforts to streamline MLAT processes, for example by updating MLATs to cover modes of communications associated with evolving networks and services, and to ensure that they constitute timely and efficient means of accessing data. ACTO members believe that policy framed for data security should be data-driven, based on empirical evidence of a specific harm, and be adaptable both over the time and cross-border keeping in mind it is global in nature.

Cross-border data flows have also been a driving force behind the emergence of so-called global value chains in which businesses' operations are fragmented across borders in order to increase efficiency, lower costs, and speed up production. The flow of data is as important as the movement of goods. Data needs to move to create value. Data sitting alone on a server is

like a static /storage library where it's information flow is restricted and against value addition to foster innovation.

The growth of the Internet has also entailed the growing ability of people, businesses, and governments to collect, share, and use data across borders. The development of new technologies, products, and services in recent decades would never have been possible without the ability to freely move data across borders. Combining globalization with new technology and with new business models has dramatically accelerated the pace of change and innovation. The success of the cloud computing industry depends on robust protections for the privacy and security of customers' data. Consumers rightly expect that the information they entrust to cloud service providers will be highly secure and that CSPs will be respectful of their privacy. Consumers should have consistent and predictable privacy protections for the information they deem private and sensitive, no matter how or with whom they share it. Establishing this trusted environment for consumers is crucial to the success of the market, separate and apart from the policy frameworks for privacy and security issues. So if there are any gaps in addressing "specific" concerns, those need to be defined and discussed with industry to find a plausible solution which is in the interest of all stakeholders.

Governments can build trust in the cloud computing industry by ensuring that cloud service providers follow industry best practices and guidelines regarding the use and protection of personal data. The consultation paper cites the frameworks developed by the Asia Pacific Economic Cooperation (APEC), the Organisation for Economic Co-operation and Development (OECD), and the International Conference of Data Protection and Privacy Commissioners (the Madrid Resolution of 2009), which serve as widely accepted international standards for multinational companies that collect, use, and transfer data, as well as for states when facilitating the transfer of data across borders. Rather than erecting barriers to cross-border data flows, the TRAI should ensure that cloud service providers in India adhere to principles such as these and provide strong accountability mechanisms for customers and others who wish to challenge data management practices.

Seamless flows of information across borders are essential to growth throughout the global economy, since services, manufacturing, and even agriculture increasingly rely on digital communication and other data transfers. Regulatory frameworks should avoid and eliminate barriers to these data flows. Further the regulatory framework should be such that it enables the

service suppliers of other countries, customers of those suppliers, from electronically transferring information internally or across borders, accessing publicly available information, or accessing their own information stored in other countries.
