Submission on

TRAI Consultation paper on Privacy, Security and Ownership of the Data in the Telecom Sector

Submission on

TRAI Consultation Paper on Privacy, Security and Ownership of Data in the Telecom Sector

The Internet and Mobile Association of India ("**IAMAI**") is making the submission in response to the Consultation Paper on 'Privacy, Security and Ownership of the Data in the Telecom Sector' [Consultation No;09/2017]. Our response is divided in 2 sections. **Section I** gives the broad principles for proposed data protection law. **Section II** gives itemized response to the questions raised in the consultation paper.

I. Synopsis:

Section I:

1. Importance of Data Protection and Privacy
2. Digital Ecosystem
3. Impact of the regulation on the digital economy
4. Principles of regulation
5. Definitions of data
6. Obligations of data controllers

Section II:

Response to questions raised in the Consultation paper.

Section I

1. Importance of Data Protection and Privacy

i. Any data protection regulations must take into account the rights of citizens and constitutional rights of enterprises to carry on trade and commerce in India free from arbitrary and unreasonable restrictions. Equally, it is important that rights of users and obligations of enterprises be described clearly to avoid ambiguity with respect to obligations and compliances.

ii. Any policy should focus on providing regulatory certainty and consistency, preventing misuse of personal information and making companies accountable through self-regulation without being prescriptive.

iii. Considering growth of startups 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.

2. Digital Ecosystem:

We would like to submit that the digital ecosystem is vast, ever expanding and nebulous. It would not perhaps be judicious to predefine it and regulate it. Pre-definitions may restrict the growth of the digital ecosystem. We would request the Authorities to restrict the present consultation to the telecom sector alone.

We understand from news reporting quoting the Honourable Chairman that TRAI would be making recommendations to the Justice Sri Krishna Committee set-up by the Government to draft the Privacy Bill. We therefore would like to take this opportunity to make a detailed submission on the digital/internet sector in this response so as to communicate our concerns and considerations to the Experts Committee through the good office of the Authority.

3. Impact of the regulation on the digital economy

i. The economic impact of wider internet access, mobile phone usage and digitization in India is well recognized. Any measures undertaken with regard to data protection would have to factor in the economic impact of such decision for the reasons specified below:

a. Growing number of Internet and broadband connections have given the Indian economy a much-needed fillip by adding USD 17 billion to the GDP annually from the year 2012.
b. A report, jointly prepared by the Indian Council for Research on International Economic Relations ("**ICRIER**") & IAMAI has noted that as the number of internet users goes up, the growth impact of the internet will improve significantly.
c. The above-mentioned report also added that 10 per cent increase in mobile penetration can increase the GDP of India by 1.5 per cent in the next few years. [1]
d. In recognition of the positive impact of greater penetration of mobile telephony and the internet in India, the Government has launched the "Digital India" campaign to improve online infrastructure and by increasing Internet connectivity or by making the country digitally empowered in the field of technology.
e. Furthermore, with the steps taken by the Government towards digitization of the Indian economy such as the Unified Payments Interface ("**UPI**"), the

[1] http://www.business-standard.com/article/technology/internet-penetration-to-boost-india-s-gdp-112012000083_1.html, last accessed on September 15, 2017

demonetization scheme, the "Rupay Kisan Card" scheme, the Unified Mobile Application for New-Age Governance program ("**UMANG**"), the Targeted Public Distribution System ("**TPDS**"), the PAYGOV INDIA Scheme and the measures such as the exemption of miniature Point of Sale ("**POS**") and micro-POS machines from Countervailing Duty ("**CVD**") and Special Additional Duty ("**SAD**") in the 2017-2018 budget[2], the dependence of the economy on the penetration of mobile telephony and the internet in India has increased decisively.

f. In addition to the above, India is also currently the home to the third largest number of technology driven startups in the world with over 4,750 technology startups, with almost 1,400 new start-ups being founded in 2016.[3] It is relevant to note that such startups are thriving in India due to the ability to access a large and varied database of information with provides such companies with the ability to innovate and address the latest demands and needs of consumers in India. Additionally, such technology based startups also positively impact India's economy and are expected to raise US$ 800 million in 2017.[4]

g. The Government, whilst recognizing the positive impact of startup's to the Indian economy has also launched the "Startup India" campaign based on the "Startup India – Action Plan" wherein, it is actively promoting bank financing for start-up ventures to boost entrepreneurship and encourage startups with jobs creation in India. The Government, in furtherance of this campaign has launched "iMADE", an app development platform aimed at producing 1,000,000 apps in India to build an indigenous Digital ecosystem.

ii. We would like to highlight that any form of over-regulation may adversely affect innovation, creativity and competition in the concerned sector and will serve as a barrier to setting up of new internet / mobile telephony based businesses and services along with adversely affecting the growth of the technology based startup sector in India. Resultantly, the GDP of India may also be adversely affected.

iii. Therefore, any recommendations by the TRAI must create a right balance between economic growth social development, users' interest and tech innovation.

[2] http://www.businessinsider.in/Liberalization-in-the-FDI-policy-to-favor-several-e-commerce-companies-in-India/articleshow/57254926.cms, last accessed on September 18, 2017

[3] http://indianexpress.com/article/technology/tech-news-technology/india-worlds-third-biggest-tech-startup-hub-study-2988745/,last accessed on September 19, 2017

[4] https://www.ibef.org/economy/indian-economy-overview, last accessed on September 19, 2017

4. Principles of regulation

i. *Prevention of harm principle*

a. The principle purpose of data protection should be towards preventing misuse of information and harm to consumers rather than overregulating entities involved in collection, processing or storage of information.

b. Remedies for breach should be designed to prevent harm resulting from wrongful collection or misuse of personal information.

c. Such remedies should also be proportionate to the likelihood and severity of threatened harm to the consumer.

ii. *Technology neutral*

The regulatory approach needs to be technology / platform neutral to facilitate the growth and development of technology whilst simultaneously protecting the rights of consumers. This will also ensure that any regulation in this regard is not rendered redundant in light of technological innovation.

iii. *Principle-based regulation*

a. The data protection framework should be looked at a from a holistic perspective, i.e. should take into consideration the interests of industry players, recognizing that considerable number of small and medium sized enterprises are engaged in the digital economy and collect / process data in various forms and therefore any prohibitive / onerous obligations will stunt the growth of the sector. Expeditious and pragmatic measures should be preferred over a dogmatic and bureaucratic regime that may cripple business and innovation.

b. Regulatory measures must be simple for compliance, consistent and uniform in its interpretation and predictable in its application.

c. The TRAI has already recognized the merits of a self-regulatory approach in its 'Recommendations for Cloud Services'.[5] Given the peculiarities and nature of digital services coupled with technological developments, such an approach would also be conducive in relation to digital services. The industry has time and again shown maturity and responsibility in addressing concerns of not only the government but also users.

[5] Available at: http://www.trai.gov.in/sites/default/files/Recommendations_cloud_computing_16082017.pdf

d. Market / industry driven practices should lead to industry players voluntarily adopting higher standards of data protection and measures to prevent breach of public / consumer trust.

e. Whilst entities may be allowed to self-regulate, they should also be held accountable for breaches / violations / loss caused to users. A liability may be enforceable against such entities when such breach results in losses to the user.

iv. *Consent cum rights based approach*

a. The data protection framework should imbibe a combination of a rights and consent based approach. Appropriate balance is needed, keeping in mind various perspectives: Sensitivity of information/transaction, Consumer Behavior & Convenience and Legitimate interests.

b. Entities should ensure that data collected from users is proportionate to the purpose. They should abide by basic principles such as transparency, accountability, prevention of harm, and dialogue with the user.

c. Whilst consumer consent should be taken by entities collecting certain forms of identified sensitive data, non-sensitive forms of data should be less regulated. Creation and handling of pseudonymized data should not be subjected to any consents.

d. The industry recognizes that context may determine the nature of information and an individual's privacy may attach to some information while it may not to other information, therefore regulation needs to allow for such flexibility. Further, consideration of consumer behavior such as a consumer's unwillingness to provide numerous consents at each instance for every kind of data, also would need be taken into consideration before any regulatory approach is finalized. The TRAI has, itself recognized the importance of the consumer's user experience whilst using a service, therefore the end user's experience of using a product should also need to be factored in any regulatory approach in this regard.

e. Consent need not be looked in isolation but with other principles like transparency, access and Prevention of harm as espoused in 4.i.

f. As a separate but related point, government and private parties should collaborate to create consumer awareness.

v. *Free flow of information*

a. Cross border data flow is essential for international trade and commerce. The basic premise of the digital economy is that it blurs traditional boundaries of borders.

b. Restrictions on the cross-border transfer of data should be avoided. Data localization requirements, if any, should not be imposed solely on the ground of protectionism. Unreasonable restrictions on usage of data may be prohibitive and would be counter-productive in providing Indian's with simultaneous access to the world's best technology and products especially in the context of development of a cash-less and digital economy.

c. The data protection framework should not create unnecessary barriers to cross-border information flow, including administrative and technology restrictions for businesses.

d. To enable cross border transfers, nations should develop framework for mutual recognition / acceptance of cross border privacy rules. Cross Border Privacy Rules under the APEC Privacy Framework should be considered. The Indian Government should ensure that it has access to data generated in India but located / stored in foreign countries with due reciprocity.

vi. *Innovation booster*

a. Data should be a facilitator for innovation and ideas for startups and medium and small enterprises in the digital services space. Value is not attributable to the data itself but rather the insight derived by businesses from such data resulting in betterment / new products and services, possibly resulting in a high quality of life for the user.

b. Collecting entities should be given the freedom to use such anonymized/ pseudonymized data collected from consumers for innovation, analytics, commercialization, research and development and on other grounds, without having to obtain specific consents from the consumer.

vii. *Accountability of service providers*

a. The industry recognizes that consent of the data subject (users) should be paramount in the collection and processing of their sensitive data. The user should be empowered to control their sensitive data and the purpose for which the same is collected. However, the focus of the regulation should not be on imposing restrictions on the collection of data, but rather it should be transparency, accountability and on preventing the misuse of data and a strong redressal mechanism.

b. Entities should be responsible for their actions and the outcome of their actions, without restricting trade and innovation.

c. Further, such a regulatory approach would result in less administrative costs and hassles for entities and would be in furtherance of the Government's initiative to make doing business in India easier.

d. A user should be notified of a data breach wherever relevant, along with relevant details and access to a grievance mechanism.

5. Definitions of data

i. The need of the hour in order is to formulate a balanced and reasonable data protection regime whilst balancing the right to engage in inter-state trade and commerce under a reasonable, consistent and predictable regulatory regime, whilst keeping in mind the economic impact that such a regime has in India.

ii. It appears from the Consultation Paper that TRAI has placed all types of information, irrespective of the sensitivity, in a single bracket of information and has suggested a single standard of protection for such information in India. Such a broad definition for information may not be consistent with existing law under the Information Technology Act, 2000 ("**IT Act**") and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("**Data Protection Rules**") or the observations made by the Supreme Court. For example, if a single broad definition for information is adopted, an entity that is only obtaining the name and phone number of an individual would be expected to provide a standard of data protection similar to that of an entity which is collecting and processing health and financial information of individuals. These entities are not collecting the same kind of information and thereby should not be obligated to adhere to the same standards of data protection.

iii. Such a data protection framework may be brought about by adopting specific and contextualized definitions for different kinds of information based on the sensitivity of the information and prescribing the standard of protection afforded to such information proportionately. Therefore, it would be advisable for a regulatory regime to segregate / classify data based on the sensitivity of the data along with the purpose of usage of such data and specify that different categories of data should have different levels of

compliances / protection such as opt in versus opt out, consent requirements, purposes for collection / use, data sharing and transfers.

iv. Such a segregation is already in place under the IT Act and the Data Protection Rules wherein "SPDI" and "Personal Information" have already been categorized separately as provided above. Adequate revisions may be made to such definitions and the data protection framework for each category may strengthened based on the observations made by the Supreme Court in the Privacy Case, wherein the Supreme Court has held that the right to privacy is a fundamental right under the Constitution of India. The Supreme Court in its judgment has opined that while the definition of personal information adopted by the Government in the new data protection framework should provide legal certainty, it should at the same time provide for proportional treatment of information / data based on the nature of such information / data.

v. Additionally, from the Consultation Paper, it appears that one of the objectives of TRAI is to put in place a data protection regime to specifically regulate the data analytics industry in India. However, it should be noted that information that is processed by the data analytics industry is primarily anonymized and de-identified and to that extent may not be capable of identifying individuals. Processing of such information results in no harm to the user and in fact is often times used for the development and provisioning of improved services to them.

vi. Ultimately, in formulating a data protection regime, it will be important not to lose sight of the rights of 'users' in respect of their personal data including the ability to easily and without cumbersome & self-defeating processes transfer their data ('data portability'). Equally, controllers and data subjects should not be viewed as having opposing interests but rather as being part of a dynamic and mutually beneficial relationship.

Therefore, it is submitted that it would be advisable for the appropriate authority to not include such information under the definition of "Personal Information" whilst formulating the new data protection framework to ensure that framework, does not become overly restrictive for the data analytics industry in India.

6. Obligations of data controllers

i. The concept of a 'data controller' and their roles and responsibilities should be clearly defined.

ii. The user / the individual providing information (personal information or sensitive personal information) should have control over the access, use, transfer, disclosure of such information to the extent permissible by law. The individual should be in control of her / his own data.

iii. Any proposed regulation should define the broad guidelines on the basis of which entities should self-regulate and perform regular audits, checks and balances to ensure there is no misuse of information procured. Recognizing that informational privacy rights of an individual are paramount, sharing such information, should only be under authority of law, in accordance with principles laid down by Supreme Court

iv. The APEC Privacy Framework[6] ("**APEC Principles Framework**") is a framework which aims at promoting electronic commerce throughout the Asia Pacific region and is consistent with the core values of OECD's 1980 Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data (OECD Guidelines). The APEC Principles Framework provides that the entity that collects the information / instructs a person to collect information is the personal information controller and is responsible for ensuring compliance with principles such as:

a. Preventing Harm principle: preventing harm / misuse of the personal information and the consequent harm to individuals;
b. Notice principle: providing a notice to the users to ensure that individuals know what the purpose of collection of information;
c. Collection Limitation principle: information should be collected only for the purpose that it is required for and the proportionality to the fulfilment of such

[6] http://publications.apec.org/publication-detail.php?pub_id=390; A framework which aims at promoting electronic commerce throughout the Asia Pacific region and is consistent with the core values of OECD's 1980 Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data (OECD Guidelines).

purpose may be a factor in determining what is relevant. Further, such collection method must be lawful and fair.

d. Use of Personal Information: Collection of personal information should give regard to the context and intended use of such information and it should be with the express consent of the provider of such information.

e. Choice: Users should be provided with clear, prominent, affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information.

f. Integrity of Personal Information: Personal information should be accurate, complete and kept up-to date to the extent necessary for the purposes of its use.

g. Security Safeguards: Controllers should protect the personal information that they hold with appropriate safeguards against risks such as misuse / unauthorized use or modification.

h. Access and Correction: Individuals should have the ability to access personal information and challenge the accuracy of information relating to them with the controllers.

i. Accountability: A controller should be accountable for complying with measures that give effect to the principles stated herein above. Upon transfer of information to third parties, the controller should obtain the consent of the information provider and take reasonable steps to ensure the organization adheres to such principles.

v. Consistent with the APEC Principles Framework, there must be broad principles that act as guidelines, which are binding on data controllers. The onus to prove compliance with the adopted internal policies should lie with the controllers and they must be held accountable for any violations.

vi. A distinction needs to made between Data Controllers and Data Processors, which often are different parties. While Data Controllers collect data directly from users and are thereby responsible for following various guidelines of data collection, the data processors are only contractually obligated to the data controllers and special provisions needs to be made to absolve them of certain responsibilities/obligations that would otherwise apply to data controllers. This is especially important for the IT/BPO/Cloud businesses that form the bulwark of the IT/ITES service sector in India.

Lastly, while principles may be provided for self-regulation, the data protection framework that is to be adopted could be a combination of a rights based and consent based approach. Such an approach could recognize the right of the user to consent to the collection of the data, but should also lay down that the data should be handled in line with board principles as stated herein above.

We have provided below, question wise response to the questions raised in the Consultation Paper.

Section II

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?

The Supreme Court in the Privacy Case has recognized privacy as a fundamental right vis-à-vis state, which can be restricted only upon following the procedure established by law. The Supreme Court has also provided several observations in relation to the informational privacy in the hands of non-state entities. In view of the observations made therein, the Government is required to enact a broad data protection law. MeitY has appointed a committee headed by Justice BN Srikrishna to provide recommendations on data protection in India.

It is preferable if the proposed data protection framework is formulated holistically, rather than sector wise. Furthermore, in order to ensure that there is no additional uncertainty brought about, the Government should not carry out any amendments to the current data protection framework pending implementation of the proposed data protection law. Such actions would bring about uncertainty in the industry along with imposing additional compliance obligations for the industry, in the interim period.

At present:

- State action is governed by the ruling of the Supreme Court in the Privacy Case.
- Internet access services as provided by telecom service providers ("**ISPs**") are governed by Indian Telegraph Act, the licensing agreement and the IT Act
- *Internet content* services as provided by internet companies are governed by the IT Act.
- Users of internet services are protected under the IT Act and Data Protection 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 telecommunication service providers and licensed services.

IAMAI Suggestion: *Following the recent Supreme Court directives and taking into consideration the ongoing process in MeiTY, it is expected that a data protection framework will soon be introduced. This Consultation Process initiated by TRAI is best suited as a feedback in the MEITY process. Once the data protection law is enacted, TRAI should review the existing provisions in the Indian Telegraph Act and licensing conditions to recommend changes to the Department of Telecommunications ("**DoT**") to align with the new requirements. DoT/TRAI could also issue advisory or guidelines for the telcos to comply with these new requirements.*

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?

Definitions

The existing IT Act and the Data Protection Rules define the term 'data', 'personal data' and SPDI. Rule 2(1)(h) of the Data Protection Rules defines "personal data" as data which directly identifies a person or can be connected with other data to indirectly identify a person. Only certain information is classified as SPDI viz "*passwords, financial information, physical, physiological and mental health condition, sexual orientation, medical records and history and biometric information.*"

It can be evaluated whether additional sets of data should be included in the definition of SPDI.

Furthermore, the definitions as provided for 'personal data' and 'SPDI' under the Data Protection Rules and the IT Act are in line with internationally accepted norms with regard to data protection. Such classification of data is followed in the United States, most European countries, Australia, Singapore, Japan, and others.

Additionally, the recently proposed General Data Protection Regulation ("**GDPR**") for European countries has expanded the definition of 'personal data' to include online identifiers, location data, and genetic information. It should be noted that online identifiers and location data serve necessary purposes such as enabling online advertising, without which the internet would no longer be a free resource. Given that the processing of anonymized data generates a majority of

the value associated with data without any adverse impact on the user, the data protection framework being envisaged should incentivise the processing of such anonymized data over 'SPDI', where appropriate.

In addition to 'personal data' and 'SPDI', a few more classes of data are gaining legal recognition globally, such as 'anonymous data', 'pseudonymous data' and 'big data'. The Right to Privacy Bill, 2011 had taken steps towards ensuring that the data protection framework in India is inclusive of such global practises by providing a definition for the term 'anonymized'.

Consent

The data protection framework in India is based on the principle of informed consent. As per rules 4 and rule 5 of the Data Protection Rules, any entity / individual which is collecting / processing SPDI is required to have in place and display clear and unambiguous privacy policy detailing how the data that it collects / processes is used. Furthermore, no entity / individual may collect / process data without obtaining the voluntary, written consent of the concerned individual along with providing them with the relevant details of the people responsible for the security of their personal data.

Once various types of data are appropriately classified, it would be prudent to try for a right and consent based approached as discussed in para 4 (iv) of the introduction. The aspects for which the consent ought to be obtained should be clearly identified e.g. for data analytics / creation of big data, as such consent may not be required.

The obligation to obtain relevant consent ought to be only on the data collector or other data processors who want to use the data for additional purpose than one communicated by the original data collector.

IAMAI suggestion: *Any proposed legislation should explicitly recognize the role that purpose, context and proportionality (including voluntary disclosure) play in determining whether a particular piece of information in isolation or in combination with other information constitutes personal information. The definition of personal information should provide legal certainty, but as recognized by the Supreme Court in the Privacy Case, it must also apply to various contexts and be applied proportionally.*

New data protection framework, should not become overly restrictive for the data analytics industry in India. Singapore and Japan, wherein anonymous processed information, which is information obtained from personal information that is not capable of identifying a specific individual may be

transferred freely without obtaining consent, provide a good reference point when it comes to dealing with anonymized data.

In addition, it would also be preferable if an inclusive definition for 'data' is provided in order to ensure that the definition that is adopted is not restrictive and to account for future technological developments and advances. The law should recognize market/industry driven developments that have led to increase in user transparency and trust.

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.

As stated above in point 6 of the introduction, the rights of a data controller may never supersede the rights of a data subject, unless it is for reasons of national security or mandatorily required in public interest. The data subject's consent should always be procured except for legitimate interests for the usage, access and storage of information provided to the data controller / service provider.

Stages of data being handled:

There are broadly 2 stages of data being handled: first being data in transit (from the data subject to the designated data controller which in turn is often handled by a third-party data processor) and second being, data after completion of transit, i.e., once it reaches the hands of the data controller. While ISPs are exposed to data in transit, users (through their devices) have control over data once it reaches the data controller / digital service provider. Thus, any personal data can have multiple 'Data controllers' depending on the usage of such data by the users.

As stated in point 6 of the introduction, the 'Rights and Responsibilities' devised for 'Data Controllers' need to framed keeping these distinctions in mind.

Any Conflict?

Data controllers and data subjects are not in conflict. The rights of one do not supersede the rights of the other. Data subjects voluntarily offer their personal data for the convenience of customised services, and data controllers profit from providing those services. It is symbiotic relationship in which both parties are winners. While the rights of data subjects / users are enshrined in the Data Protection Rules, the rights of data controllers must be expressly set out in the proposed data protection law. Furthermore, the current copyright laws should recognize the rights of data controllers with regard to proprietary rights over datasets.

Some best practices

As elaborated in point 6 of the introduction, the APEC Privacy Framework is a business friendly and user centric framework which also supports cross border data flows and should be considered when formulating the law. It recommends privacy principles of Preventing Harm, Notice, Collection Limitations, Uses of Personal Information, Choice, Integrity of Personal Information, Security Safeguards, Access & Correction and Accountability. The principles of *Preventing Harm* and *Accountability* particularly standout for being pragmatic and outcome focused by making organizations responsible without stifling trade and innovation. In addition, these principles are informed by the Fair Information Practice Principles ("**FIPPs**") and the OECD principles and were drafted with the digital economy in mind.

It must be noted that since various service providers' gain access to personal or sensitive personal data, which is shared by a user in order to use applications / websites, these ISPs may use such information shared in a manner that is not consented to by the provider. This, in many cases leads to creation of user profiles and use of cookies on browsers to track user behavior. In many cases, the information shared by the user may be used for advertising and promotion purposes (which aids monetization and thereby enables offering digital services at affordable rates), without the express / informed consent of the data subject. Therefore, in order to empower the user with regard to her / his data as well as retain the functionality of the service, a rights and consent based approach must be adopted.

IAMAI Suggestion: *Instead of prescribing privacy practices in form of administrative requirements, the privacy framework should define the broad principles and requirements and allow organizations to design their own privacy programs that could be based on due diligence guidelines. Industry specific self-regulation could be encouraged. Any legislation needs to be backed by an adequate implementation ecosystem (institutional capacities and capabilities, industry self-regulation, effective grievance redressal system, user awareness, active civil society, and research) to be truly effective.*

While organizations should be allowed to self-regulate (based on the outcome based guidelines), they should be held accountable for any violations. In case of any breach or complaint, the onus to prove due diligence should lie with the organizations.

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?

Market regulations should be based on evidence. Any restrictions on the free flow of data such as an 'audit' mechanism is only going to hamper innovation and the free flow of information and data. Such a mechanism could also be prone to misuse in the wrong hands and could potentially expose the user information of millions of data subjects who would be trusting their information with the content providers. The proposed architecture could also be very expensive to develop and regulate. Considering that new internet enabled services are popping up every day, especially overseas, it would become cumbersome to calibrate the system to ensure the 'audit' of all services to which Indian customers submit their data. It is therefore suggested that any enforcement for breach of data be 're-active' as opposed to 'pro-active' as the cost of pro-active enforcement are too large.

Data harms can be classified into three broad heads: discrimination harms (when a user's race, gender, or other such protected category is divulged or inferred by algorithmic data correlation), privacy harms (personal data becoming known despite the use of privacy-enhancing techniques such as de-identification), and security harms (sensitive data being breached or non-consensually shared).

The tech platforms are already building capabilities to empower users to better understand their PI usage, and control their data. The authorities on their part can help generate greater public awareness about the kind of harms that public can face so that they are enabled to make better informed choices. In the Indian context, creation of public awareness is a necessity and instituting data awareness programs for the public would go further in improving personal data security as opposed to setting up an architecture to actively monitor and audit data controllers.

IAMAI Suggestion: *It will be extremely difficult or perhaps impossible to create a pro-active auditing mechanism which can audit the use of personal data and associated content. It is instead suggested that the government take steps to educate the general population on good cyber security habits and create awareness on the sharing of personal data. Considering that a large portion of the internet using population in India is very new, there is an urgent need to spread awareness of good internet habits. Building understanding among users through education and awareness, making organizations accountable through self-regulation and strengthening grievance redressal mechanisms to empower users would be a more cost-efficient and effective way of achieving the same objective. International recognized standards for security of data may be adopted.*

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?

The Government has placed a lot of emphasis on start-ups and India is home to the third largest number of start-ups. It would be important to create a regulatory framework and environment which is conducive for the growth of these and more start-ups. Excessive compliances and regulations would be counter-productive to the growth of the digital economy. Protection of rights of users (addressed in response to Q 2 above) and growth of the digital economy need not be mutually exclusive.

Consistent and unambiguous definitions – clearly setting out principles with no room for arbitrariness in approach or discretion in application will help engender the right ecosystem for creation of data based businesses.

As the Supreme Court in the Privacy Case has also noted that rights attached to information would also depend on the context and hence, a regulatory framework should avoid a prescriptive and absolutist approach. Keeping these considerations in mind, it is important that monetization of data should be possible. The differing levels of sensitivity or threat perception if the different forms of data, care must be taken to allow monetization based on certain forms of data (like 'metadata') so as to ensure affordable internet services for the extremely price sensitive Indian customers while at the same time allow breathing space for the fledgling Internet sector developing under Digital India and Start-up India initiatives.

Going forward, sectors like Big Data Analytics, Artificial Intelligence (AI), IoT, M2M etc. will all depend on access to data and these sectors are the future of digital technology and industry, with potentials of major contributions in terms of GNP, employment generation etc.

Thus, care must be taken to ensure that Privacy rules do not impede technological innovation and consumer interest in terms of access to high quality goods and services for a reasonable cost. Along with the significance of sharing and monetization of data for startups, this is critical to have greater penetration of digital services in India while at the same time to ensure development of an indigenous internet service sector which has the potential of replicating the IT/ITes sector's success in the near future.

IAMAI Suggestion: *A regulatory framework must be simple for compliance, consistent and uniform in its interpretation and predictable in its application. The framework should recognise the huge economic potential in India and that regulations should not stifle innovation and growth of the digital economy. The public policy focus should be on providing regulatory certainty and consistency,*

preventing harm to users, misuse of PI and making companies accountable through self-regulation without being prescriptive. It should focus on building an adequate implementation ecosystem, including institutional capacities and capabilities, industry self-regulation, effective grievance redressal system, user awareness, active civil society, and research. These mechanisms will enable a stable ecosystem for business innovations based on consumer requirements that will help the growth of new data based businesses in the coming days.

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?

The value of data is not linked to the data itself but is derived from the insights and analytics from the data. Driven by competition and market standards, each entity should possess its own strategies and measures for innovation in order to better / introduce new product offerings, based on user data it has access to. It is the innovation, ideas and data products that distinguishes businesses from each other. If the Government compels such entities to provide access to such data and if such data is made accessible to competitors in a common sandbox, the incentive to innovate may be lost. Such an act, i.e. compelling businesses to render the Government access to their data for use in the sandbox may result in violation of rights guaranteed under Article 300A of the Constitution and fundamental right to trade under Article 19(1)(g) of the Constitution.

Indian businesses have in the recent past innovated and developed cutting edge technology and know-how to India, and are even competing on the world stage against global renowned players. The data protection laws should be conducive to such innovation and should not hamper the growth of start-ups entering the playing field with new ideas.

IAMAI Suggestion: *The Government may set up a data sandbox if it so desires, but only if entities can participate on a voluntary basis and only if the data that is shared on such a data sandbox is raw data and not processed or analyzed data. Simultaneously, the Government should incentivize private parties to set up their own sandboxes via collaboration with such private parties including by way of a 'public-private partnership'. The output attained from such sandboxes could be made open source. At the same time, the Government should continue to promote publication of data by government agencies under the open data policy [ex. data.gov.in].*

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?

The global experience in data protection points to the most successful regimes being those based on a voluntary compliance based model as has been seen in the APEC Principles Framework as has been described in detail above. Such a model works on the basis of compliance, incentivization and swift enforcement which in turn leads to a general increase in compliance levels due to market forces and adoption of best practices to stay competitive.

This open structure of global data protection regime has been one of the major reasons why Indian IT companies have been able to service global clients and become a leader in the data outsourcing space. Therefore, it is essential such a reciprocal model is also applied by the Indian government. Any kind of technological monitoring runs the risk of resulting in a geo-fencing of sorts of global data, and should therefore not be used as a means to insist on data localization which would be detrimental to the entire digital and internet sector in India. Further, given the pace at which technology evolves, we believe that any technological solution implemented by the Government runs the risk of becoming redundant / obsolete very soon.

IAMAI Suggestion: *Therefore, the Government should explore a self-regulation model where the industry as a whole act to voluntarily adopt global best practices and the Government retains the power to intervene only if it believes that there is a failure for market forces to act. The legislator should be encouraged to recognize and endorse a culture of corporate accountability. Given the peculiarities and nature of digital services coupled with technological developments, such an approach would also be conducive in relation to digital services. The industry has time and again shown maturity and responsibility in addressing concerns of not only the government but also users.*

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?

Data encryption is the key for any safety and security measure for telecommunication infrastructure. To ensure Privacy of data, India needs suitable data security policy that is able to protect all the states of digital data. In India 40 bit standard is required to be adhered to by the companies as per the ISP license agreement and any bit length more than 40 will require prior approval of the government and handing over the encryption keys. Similarly, RBI/SEBI mandates usage of 64/128 bit.

Not all internet companies require the same standard of encryption given the fast pace at which technology is changing. For instance, internet trading and banking would require different levels of encryption than the social media companies. Another example is of Aadhaar database which

uses highest available public key cryptography encryption (PKI-2048 and AES-256) as it is a critical information infrastructure. Hence if the encryption upper limit is mandated to a common single benchmark or standard, it would not be appropriate.

Any measure must be technologically neutral and compatible with international standards. A framework should not be for a particular technology but should set out principles and enforcement mechanisms.

Encouraging industry to participate in setting standards and adopting a co-operative approach to regulation would also be a helpful measure.

IAMAI Suggestion: *There should be freedom of encryption as per the users' requirements and there should not be any upper limit or particular format prescribed for using encryption. Rather from the cyber security and privacy angle the rules can specify a lower limit that is essential to protect data.*

For the digital ecosystem, a suggestive over-arching policy framework would be

- *Empowering users by giving them control over their data; recognizing the industry efforts in this direction which are based on brand safety and competition*
- *Not restricting collection of data but focusing on misuse of data and preventing harm*
- *Making organizations accountable through self-regulation without being prescriptive*
- *Building capacity of users through education and awareness*
- *Strengthening grievance redressal mechanisms instead of proactive monitoring*
- *Technology neutral measures and self-regulatory mechanism*

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?

As a regulatory authority for telecom services providing internet access only, devising mechanisms to control other stakeholders like content providers and application service providers may be an overreach for the Authority and perhaps is best avoided. There should be a neutral data protection law that could be applicable across various industries and service providers which puts the users in control of their information such that it does not in any manner hinder the functionality of the service.

Tech platforms today are already including concepts of express consent and "opt-in" / "opt-out" mechanisms in order to allow the users to control the usage and access to their information, be

this personal information or sensitive personal information. Users should also be made aware of the consequences of parting with their data for availing the services, especially where the data may be used for an organization's marketing or advertisement purposes. The data protection law should focus on creating awareness amongst users and make organizations accountable through self-regulation.

Further, there must be distinction drawn between the roles and responsibilities of a data controller (entity that collects the data and uses such data based on the purpose) and a data processor (entity that processes the data on behalf of a data controller) as stated in point 5 of the introduction and our response to Q 3 above.

As elaborated above in Q.1, the Supreme Court in its judgment in the Privacy Case has provided certain observations with regard to 'informational privacy' in the hands of non-state actors. The judgment also mentions various aspects of collection, use and handling of data, such as big data, data analytics, use of wearable devices and social media networks resulting in generation of user data to end users' lifestyles, choices, preferences and for tracking user behavior and for the creation of user profiles[7]. These broad observations must be taken into account while framing a neutral data protection law to ensure the right of privacy of an individual is recognized as also recognize the right of the individual to transfer such data freely, without unreasonable hindrance.

Some of the issues in data protection being discussed around the world include:

Data portability

- Unlike the right of access, which applies to human-readable data, data portability requires machine-readable data to facilitate interoperability.
- To prevent data portability from impinging on the rights of data controllers, it only applies to personal data which the user knowingly submitted to a data controller.
- According to the Article 29 of the Data Protection Working Party, European Commission[8], data portability does not extend to data held by third parties, derived data, or data obtained while the user was passive, such as tracking.
- Hence, anonymised, proprietary datasets, including those which contain behavioural data, are not covered by the right to data portability.

[7] http://www.nishithdesai.com/information/news-storage/news-details/article/supreme-court-holds-that-the-right-to-privacy-is-a-fundamental-right-guaranteed-under-the-constituti.html

[8] Adopted on April 4, 2017.

- While the principle of Data Portability for Users is a welcome initiative, care must also be taken about concerns of how such provisions can harm start-ups and thereby innovation, and raise operational costs of digital service providers.[9]

The Internet of Things

- For the IoT to flourish, the 'notice and consent model' must be modified to allow simultaneous data sharing.
- The principles stated in Q. 3 read along with point 6 of the principle based submissions above, including collection and purpose limitation principles must be modified to allow large-scale collection and repurposing with narrow exceptions.
- Data security and disclosure must be completely reimagined.

IAMAI Suggestion: *The Government must complement the overall framework of data privacy to be formulated to ensure that some of the aspects of the issues mentioned above that fall under their purview are suitably addressed.*

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?

At the outset it must be set out that the role of TSPs and other communication service providers like VOIP / Messaging services are not similar. It has been recognized that VOIP / Messaging services and PSTN / UL are fundamentally different categories of services. Further, TSP/ISPs and internet service providers are different categories of 'Data Controllers' as explained in response to Q3, especially given the fact that they may be collecting different kinds of information.

While a general data protection regime will cover all forms of data breach whether by an OTT Player or a TSP, given the difference in the form of service and nature of data entailed, TSPs and VOIP service providers cannot be clubbed together given the inherent physical, technological and legal difference.

A technology/platform neutral data protection law which applies horizontally across the ecosystem should be the path forward, with each sector/category having any additional specific requirements that it may need / require from a national security or such similar perspective.

[9] Peter Swire and Yianni Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72 Maryland Law Review 335, 379.

IAMAI Suggestion: *Once a common data protection law is enacted, the TRAI may evaluate the existing provisions in the Indian Telegraph Act and licensing conditions to recommend changes (if any) to the existing regime to prevent duplication.*

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?

Exceptions in the form of differential liabilities for each entity of the ecosystem (as discussed in details in response to Q.9) need to be built in to ensure efficiency of the entire digital ecosystem.

The Right to Privacy, (including informational privacy) has been recognized as a fundamental right by the Supreme Court of India in the recent judgment in the Privacy Case. Therefore, any action by the state will be tested against the principles established by the Supreme Court.

Deeming the Right to Privacy to be a part of the right to life and right to personal liberty, Justice D.Y Chandrachud held in his judgment in the Privacy Case:

> *"An invasion of life or personal liberty must meet the three-fold requirement of (i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them"*

The Supreme Court has recognized exceptions for *inter alia* compelling state interest, national security, and the reasonable restrictions enumerated in Article 19 of the Constitution including, public order, morality and obscenity, maintaining friendly relationships with other nations etc.

Thus, any law or any action of the state that requires TSPs or any non-state actors to divulge personal information to the state will have adhere to abovementioned principles.

The government has a duty to protect national security and public safety and businesses fully recognise this aspect. Compliance with legally-valid government requests for user data is the default position of most data controllers and internet content providers operating in India have always complied with LEAs in this regard.

IAMAI Suggestion: *Any Privacy law must take into account the various degrees of liability of each agent of the ecosystem and the legal provisions should provide suitable exception of liability for each accordingly. Furthermore, any exceptions to the law should be built into the law in order to satisfy the tests laid out by the Judgment. Such exceptions should be restricted only for critical purposes*

such as national security or law enforcement and should conform to global best practices. A mechanism should be built into the law to ensure that the exceptions are not applied in an ad hoc manner and are applied with a uniform standard without discriminating among service providers. Further, 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 privacy law which exempt the data controllers and data processors from any civil liability for loss of customer data after it is handed over to the authorities in line with any of the exemptions under the law.

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?

In the globalized world, cross border data transfer is inevitable. Geographically-based regulation will naturally come into conflict with the fact that geography matters less in a business and technological sense than it used to.

Currently the flow of sensitive personal data is regulated by the IT Act and Data Protection Rules, which impose an obligation on the data transferor to contractually ensure that the transferee maintains an adequate level of protection as the transferor.

Cross border data flow is not only a universal human right but is essential for international trade and commerce. The basic premise of the digital economy is that it blurs traditional boundaries of borders. Restrictions on the cross-border transfer of data should be avoided. Data localization requirements, if any, should not be imposed solely on the ground of protectionism. Unreasonable restrictions on usage of data may be prohibitive and would be counter-productive in providing Indian's with simultaneous access to the world's best technology and products especially in the context of development of a cash-less and digital economy. This could end up with India being isolated in the global space and damage India's digital economy. This can be avoided via negotiations and dialogue to arrive at a global standard rather national laws which aren't aligned.

IAMAI Suggestion: *To enable cross border transfers, nations should develop framework for mutual recognition / acceptance of cross border privacy rules. The Indian government should consider becoming a member of multi-party agreements as this will help in enhancing market access for Indian companies especially the IT industry. The Government should ensure that it has access to data generated in India but located / stored in foreign countries. The data protection framework should*

not create unnecessary barriers to cross-border information flow, including administrative and technology restrictions for businesses.

Conclusion:

Following the recent Supreme Court judgment, Privacy will now have to be enshrined as a fundamental right and legal statutes need to be formulated.

The issue of Data Protection, though intrinsically linked to the issue of Privacy, is a separate matter. In the age of digital economy, data is an asset that drives technological innovation. Any law for Privacy will have corollaries for Data Protection provisions, and regulations for digital data will be a subset of such provisions. Any such provision needs to take into account the nature of the digital sector, its socio-economic impact in the short and long run, and make suitable provisions to ensure that the growth of the sector is not stifled due to overly restrictive Privacy provisions. Given that there is no inherent conflict between PI and data products given various stages of anonymization, there need not be any conflict of interest either between Privacy concerns and digital industry requirements in formulating Data Protection laws. In fact, the digital sector can only develop on the basis of strong and competent Data Protection Laws that recognises the right of both individuals over personal data and businesses over data products. Any provision of Data Protection needs to keep this balance in consideration.