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?

No. They are not comprehensive to protect the interest of the telecom subscribers.

What are the additional measures, if any, that need to be considered in this regard?

In addition to the TSPs, the other stakeholders in the eco-system viz., content and application service providers, device manufacturers, browsers, operating systems etc. are also to be brought under the stricter data protection requirements, apart from the coverage of IT Act, 2000. The broader principles viz., National Level Privacy Principles as recommended by the report dated October 2012 of Group of Experts (headed by Js. A.P.Shah) need to be implemented comprehensively, which are in line with the international standards based on the recommendations of Organisation of Economic Cooperation Development (OECD). Thus, the existing legal framework through the Indian Telegraph Act, 1885 entails a radical revamping to ensure more comprehensive data protection requirements.

Q. 2 In light of recent advances in technology, what changes, if any, are recommended to the definition of personal data?

Apart from the existing categories and sub-categories of personal data under the IT Act, 2000 & its Rules, 2011 (viz., passwords, financial information, health conditions, sexual orientation, biometric information etc. that can be used to identify a natural person), the definition of personal data can be expanded and brought under the Indian telecom regulatory framework, by including the other categories like call details records, calling patterns, location data, data usage information, details relating to browsing, usage of Apps, etc.

Should the User's consent be taken before sharing his/her personal data for commercial purposes?

Yes. It is prudent to mandate the User's consent before sharing his/her personal data for commercial purposes. This is suggested based on the Choice and Consent (opt-in/opt-out) under National Level Privacy Principles as recommended by the report dated October 2012 of Group of Experts (headed by Js. A.P.Shah) and also based on the Federal Communication Commission enacted broadband privacy rules, 2016 in United States.

What are the measures that should be considered in order to empower users to own and take control of his/her personal data?

The users can be empowered to own and take control of his/her personal data by implementing under the Indian telecom regulatory framework the principles like Choice and Consent (opt-in/opt-out), Access and correction etc. as recommended under the National Level Privacy Principles.

In particular, what are the new capabilities that must be granted to consumers over the use of their Personal data?

In addition to the aforesaid measures like Choice and Consent (opt-in/opt-out) and Access and correction, the data controllers need to be imposed with the mandate of giving simple to understand Notice of its information practices to their users in all their services, alongwith grievance redressal mechanism on any claims of users on the same. Further, the consumers/users could be granted with the right to demand information of their respective data controllers/service providers from the records of the regular like TRAI etc.

Q.3 What should be the Rights and Responsibilities of the Data Controllers?

While diversified obligations are contemplated on the Data Controllers/service providers, the proposed Indian telecom regulatory framework should also consider on the rights and the factors discharging their duties against the consumers. For example, there should provisions on any misuse of rights by the consumers in providing consents, having access to their personal data with the Data Controllers are to be stipulated and thereby linking with punitive actions against the consumers on such misuse practices, to safeguard the operation and business interests of the Data Controllers.

Of course on the responsibilities side, there are diversified obligations of Data Controllers are being deliberated in this Consultation Paper, which includes maintaining secrecy and divulging of information, prevention of unauthorized interception of messages, openness in implementation practices/procedures/policies, accountability, limitation on collection and purpose of processing, upfront notices to the consumers etc.

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.

No. The rights of Data Controller in light of safeguarding their operation and business interests are subject to the priority rights of individuals, who provide their Personal Data, which is being the capital for the Data Controller.

Besides the implementation of National Level Privacy Principles as recommended by the report dated October 2012 of Group of Experts (headed by Js. A.P.Shah), the Data Controllers are to be subjected to the regulatory audits through regulators like TRAI or any delegated authority.

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?

As discussed above, it is superlative to create a technology enabled architecture to audit the use of personal data and associated consent to have methodical check and balance on the activities of Data Controllers, under the proposed Indian telecom regulatory framework.

Will an audit-based mechanism provide sufficient visibility for the government or its authorized authority to prevent harm?

Taking into account the huge volume of personal data of individuals involved, audit-based mechanism would be more suitable to provide sufficient visibility for the government or its authorized authority to prevent harm to the users of Telecom sector.

Can the industry create a sufficiently capable workforce of auditors who can take on these responsibilities?

In such significant framework of the economy, sufficiently capable workforce of auditors can be sourced through the statutory professional bodies like Institute of Chartered Accounts of India, Institute of Company Secretaries of India, in order to ensure accountability of auditors.

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?

From the discussions, the factors like Choice and Consent (opt-in/opt-out) and Access and correction are to be considered as foremost measures, while implementing a technology enabled architecture on personal data usage and its associated consents.

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?

Such setup of data sandbox would certainly bring the anonymized data sets of regulated companies under the purview of the government or its authorized authority, for implementing a technology enabled architecture. Also the setup of data sandbox would enable the Government or its authorized authority and also with its approvals, the regulated companies to use such data for the development of newer services in the system.

Q. 7 How can the government or its authorized authority setup a technology solution that can assist it in monitoring the ecosystem for compliance?

The government or its authorized authority could consider creation of a technology enabled architecture on the personal data thereby bringing in all the Data Controllers viz., TSPs and other stakeholders in the Telecom sector under one roof. Such a setup could bridge the consumer consents monitoring and regulation of the anonymized data sets created by the regulated companies under a single telecom regulatory infrastructure in compliance with international standards.

What are the attributes of such a solution that allow the regulations to keep pace with a changing technology ecosystem?

Single point of control of all personal data under the telecom structure would also be characterized with research and tracking of the regulator on the new players/ changing technology in the ecosystem, resulting in upgradations in the solutions in a dynamical manner.

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?

Controlling all Data Controllers viz., TSPs and other stakeholders in the Telecom sector from a centralized watch tower /regulator and a robust legal framework for Telecom sector through an amended or reintroduced Indian Telegraph Act aligning with the other relevant statutes like Information Technology Act, 2000 etc. would strengthen and preserve the safety and security of telecom infrastructure and the digital ecosystem as a whole.

***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?**

Since there are diversified other stakeholders already marked their presence in the digital ecosystem out of the purview of legal/regulatory control, it would be a key challenge posed against the government/regulator to pull those other stakeholders within the proposed Indian Telecom regulatory framework. Rather the core issue would be as to how the data, which are already collected and being used by the other stakeholders, can be protected in light of the impugned consents that are obtained from their users hitherto.

What mechanisms need to be put in place in order to address these issues?

As discussed above, creation of data sandbox under the technology enabled architecture of personal data could be the ultimate mechanism under the proposed comprehensive Indian Telecom regulatory framework. This mechanism has to be coupled with punitive consequences in case of non-compliance.

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).

Yes. The greater parity is essential since the services provided by other stakeholders/communication service providers are not independent of the TSPs and other stakeholders acts as intermediary between the consumers and the TSPs.

What are the various options that may be considered in this regard?

Controlling all Data Controllers viz., TSPs and other stakeholders in the Telecom sector from a centralized watch tower /regulator and a robust legal framework for Telecom sector through an amended or reintroduced Indian Telegraph Act aligning with the other relevant statutes like Information Technology Act, 2000 etc.

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?

The power of exercising the legitimate exceptions could be assigned to the government or its authorized authority on the grounds of interests of public safety required in the interests of the sovereignty and integrity of India, the security of the State, public order or the prevent of incitement of offences. For Data Controller, such legitimate exceptions could be permitted under the proposed Indian Telecom regulatory framework only on requirements of any statutory compliances an not otherwise.

In particular, what are the checks and balances that need to be considered in the context of lawful surveillance and law enforcement requirements?

Regulatory reporting and audits, under the proposed technology enabled architecture of personal data for all TSPs and other stakeholders in the digital ecosystem.

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?

It is recommended that under the proposed Indian Telecom regulatory framework, necessary rules/directives could be contemplated regarding the transfer of personal data to other countries, which do not ensure an adequate level of protection. Such obligations need to be imposed on the Data Controllers, who is required to do cross border flow of information.

This is recommended on the influence of European Union (EU) Directive 95/46 read with OECD principles. EU law also includes the right to data protection at the constitutional level (for example, in the EU Charter of Fundamental Rights), and the European Court of Human Rights has construed Article 8 of the European Convention on Human Rights to include data protection.

****