ASSOCHAM SUGGESTIONS TO TRAI CONSULTATION PAPER ON PRIVACY, SECURITY AND OWNERSHIP OF DATA IN TELECOM SECTOR

We at ASSOCHAM are supportive of a collaborative approach to privacy and recommend a multi-stakeholder engagement in this direction. We support the development of privacy recommendations that promote innovation through movement of data while protecting consumer rights.

TRAI has traditionally focused on the 'carriage/transmission' layer of communications, However, this data privacy consultation covers the 'content' layer of communications.

Further two events that have occurred simultaneously – the first being the Supreme Court of India's recent ruling that privacy is "intrinsic to life and liberty" and inherently protected under the fundamental freedoms enshrined in the Indian Constitution. The second being the formation of an expert committee on data protection under the Chairmanship of Justice B. N. Srikrishna, by India's Ministry of Electronics and Information Technology (MEITY). These two events will bring in a larger debate around the issue of Data Protection and we hope that TRAI would consider aligning any recommendations to the suggestions by Srikrishna Committee.

Question 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?

Response:

We are supportive of the current legal framework which cover all stakeholders in the ecosystem including telecom subscribers and other end users. The data protection for telecom subscribers using licenses services directly from the telecom service providers is covered by the Indian Telegraph Act. The users of other services like app are covered by the protections contained in the Information Technology Act and Rules issued thereunder – specifically the IT (Reasonable Security Procedures and Sensitive Personal Data or Information) Rules, 2011 which provide a balanced and robust framework for data protection in India. In addition, various sectoral frameworks administered by various sectoral regulators such as SEBI, IRDA, RBI, and DoT apply to certain entities. Together, they act to cover the entire digital ecosystem under consideration of TRAI as part of this consultation exercise.

The current framework, as described above, has permitted the Indian digital ecosystem to flourish while at the same time ensuring end users various rights in relation to their data and defining controller responsibilities. While being conducive to innovation, the existing regime also satisfies various international benchmarks in relation to personal data protection – notably addressing issues such as notice, informed consent, use limitation, transparency, and data security – all critical aspects of privacy as touched by the Supreme Court in its recent judgment on the right to privacy. Any attempt to create a more onerous or specialized framework for India would break trend from international practices and raise barriers to cross-border data flows while degrading the ease of innovation and doing business domestically.

While considering policy issues in the sector, TRAI must be guided by the need to balance innovation, ease of doing business, and economic concerns with the need to ensure privacy and data security. A significant reason that the innovation and disruption based digital economy has thrived in India is the permissive framework afforded by the current data protection regime. We have provided further context in the responses below.

With the Indian IT Act providing a base, some of the international best practices that could be referred for balanced privacy regulations promoting cross border linkages and integration include the OECD and APEC cross border privacy rules.

The Ministry of Electronics and IT is already working on a draft of comprehensive data protection law that is expected to cover data protection in a technology and platform neutral way.

Question 2

In light of recent advances in technology, what changes, if any, are recommended to the definition of personal data? Should the User's consent be taken before sharing his/her personal data for commercial purposes? What are the measures that should be considered in order to empower users to own and take control of his/her personal data? In particular, what are the new capabilities that must be granted to consumers over the use of their Personal data?

Response:

Definition of Personal Data: As discussed in our response above, India's approach to data protection legislation must be guided by the priorities of enabling innovation, the ease of doing business, preserving the diverse character of the internet, while at the same time ensuring that privacy interests of citizens are satisfied. Within this context, it is crucial to have an appropriately scoped and robust data protection policy. At present the term 'personal information' is defined in flexible terms to refer to '*any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person'*.[1] Moreover, the IT Rules identify certain types of personal information which are deemed sensitive[2] and subject to additional safeguards. This approach is in line with international best practices and provides a balanced approach to data protection suited to the Indian ecosystem – providing a flexible approach to cover different types of personal information but providing for specific safeguards in relation to sensitive types of information. Co-opting a foreign approach to the issue would be ill-suited to the Indian setting and stymie innovative forces. As a result, there is presently no need to modify the present definition of 'personal data' under Indian law.

User Consent: Yes, consent is one potential ground for the processing of user data. This principle is recognised as part of the IT Rules which require informed consent for collection of certain types of data. However, consent is not the only valid ground on which data may be collected or processed. Requiring users to provide consent in every instance would disrupt the user experience. As long as privacy practices and policies are published by an entity (as required under the IT Rules), users must be given the choice of providing implicit consent or permitting processing on other legitimate grounds. As a result, a balanced

[1] Rule 2(1)(i), Sensitive Personal Data Rules, 2011.
[2] Rule 3, Sensitive Personal Data Rules, 2011.

data protection policy must not only recognise consent but other grounds on which processing or collection of information may be carried out. For instance, under the proposed General Data Protection Regulation which is set to take effect in the EU in 2018, consent is not the only ground for processing of data. As long as processing is 'lawful', it may be carried out. 'Lawfulness' includes cases not only where users have given consent but also the following:

(a) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(b) processing is necessary for compliance with a legal obligation to which the controller is subject or to protect the vital interests of the data subject or of another natural person;
(c) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(d) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject

Therefore, Indian framework should look to recognizing not only consent but other grounds for processing data. This especially becomes in important in cases where entities have to protect valid security or other interests and receiving consent is impractical.

***User Rights*:** Similar to the above, the regulatory approach to user rights must be carefully formulated to balance innovation, user choice, and legitimate bases for data processing. As the digital ecosystem consists of a complex interplay between various market forces, we must be mindful of the harm a wide-ranging reform would bring if not appropriately tailored. For example, a key driver of content diversity on the internet is online advertising which enables millions of websites and platforms to provide content without charging end users. Creating a restrictive data protection framework would dis-incentivise innovation and possibly starve the ability of technology companies to leverage areas like Analytics, Machine Learning etc for the wider good of society. Further this could also make many online portals unsustainable (due to the absence of ability of targeted advertising) and hence reduce the diversity of content online. Research by Catherine Tucker (MIT Sloan, 2012) shows that the EU's privacy regulation efforts have resulted in a 65% decrease in the effectiveness of online advertising. This decrease had a disproportionate impact on non-commercial websites and is likely to have effects for the diversity of content on the internet. The paper also raises the possibility that decreased levels of privacy regulation results in improved levels of consumer choice due to availability of advertising.

Question 3

What should be the Rights and Responsibilities of the Data Controllers? Can the Rights of Data Controller supersede the Rights of an Individual over his/her Personal Data? Suggest a mechanism for regulating and governing the Data Controllers.

At the outset, it must be pointed out that the optimal data protection framework will balance the rights of individuals and controllers as both sets of stakeholders have legitimate interests in the concerned personal data being processed. As such, no one set of rights should be seen as superseding or obtaining precedence over another. Users decide to part with their data in exchange for specific services or products and this element of volition and user choice must be respected.

Moreover, it must be realised that the current regulatory framework in the form of the IT Act and Rules clearly lay out rights (for users) and responsibilities (for controllers). Controllers are required to abide by various provisions of the IT Act aimed to ensure data protection and privacy (including sections 43A, 72, and 72A of the IT Act) as well as numerous obligations under the Sensitive Personal Data Rules including in relation publishing a privacy policy, use limitation, consent, limitations on disclosures, and security practices. Similarly the Rules recognise various user rights including access, review, and correction.

In other to correct this imbalance, the rights of controllers to also process user data in other legitimate manners to generate additional user value must be recognised. This would ensure business certainty and provide impetus to the development of a robust ecosystem for data-driven projects. As such, we do not foresee a requirement for special regulations which apply to regulating and governing data controllers. If nothing else, the rights of controllers to use data in innovative manners must be facilitated through appropriate regulatory intervention.

Question 4

Given the fears related to abuse of this data, is it advisable to create a technology enabled architecture to audit the use of personal data, and associated consent? Will an audit-based mechanism provide sufficient visibility for the government or its authorized authority to prevent harm? Can the industry create a sufficiently capable workforce of auditors who can take on these responsibilities?

Response:
As emphasised in our responses above, the key policy considerations that must guide a data protection/privacy framework are the ability to continue innovation in the digital ecosystem, the ease of doing business, and the legitimate privacy expectations of users in their personal information. An overly restrictive or compliance-led framework would severely impede businesses looking to innovate and originate cutting-edge data-centric products and services.

The most effective mechanism to achieve optimal compliance would be by permitting industry to evolve appropriate self-regulatory codes and certifications which provide users with comfort and confidence that their information would be safely preserved, protected, and processed in accordance with stated practices. In fact, the current regulatory framework – under the IT Rules – expressly recognises the role played by industry-led certification efforts as a method of effective compliance with the requirement to implement security practices and procedures (Rule 8).

Such a framework would be ideal as it drives compliance by harnessing market forces and incentivizes improvements in privacy. In the presence of effective certification programs, privacy practices would be driven by competition - ensuring the best possible protection for user data. An audit-based mechanism as suggested by the question would drive up compliance costs and erect barriers at a time when a key focus of the government is to improve the ease of doing business and facilitate innovative practices.

Question 5
What, if any, are the measures that must be taken to encourage the creation of new data based businesses consistent with the overall framework of data protection?

Response:
For data based businesses to thrive, the costs of doing business must be low and facilitate innovation and disruption led business models. Data protection regulation forms a key component of this framework. A balanced framework will allow businesses to flourish while an onerous framework will drive innovation outside India to more jurisdictions with more balanced regulation.

The current data protection framework only enumerates the responsibilities of data controllers without providing for their rights and the extents to which they may use user data they have acquired. In contrast, a permissive data framework which provides flexible rights to controllers to legitimately use data collected in accordance with the prescribed procedures would create business certainty and thereby ease innovation and provide a boost to the data-driven innovation ecosystem.

In light of this trade-off, the government and TRAI must encourage measures which promote innovation and competition in industry while at the same time protecting user rights. International best practices in successful data economies – such as the United States – have shown that a self-regulatory model is optimal to achieve this result. Self-regulation and certification schemes must be encouraged and the use of datasets – anonymised or not – must be permitted subject to basic transparency and accountability norms (as contained in the extant Indian data protection framework). Such a model would ensure that businesses – especially SMEs and start-ups – have the freedom to experiment with user data and evolve new models which add value to the user experience.

Questions 6 and 7 (Combined Answer)

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?

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?

Response:
Data Sandboxes: While the key objective of the government must be to protect the digital ecosystem and promote innovation, it must stop short of advocating for specific methods or types of innovation and instead leave the same to market-forces. In the absence of strong evidence of market failure, the government must not seek to promote one manner of innovative enterprise over another. While data sandboxes may be one way of promoting newer services, they should be encouraged on a voluntary/consent basis. They must not be advocated at the expense of other innovative processes or methods. Forcing companies to provide datasets for use by others would amount to expropriation of valuable intellectual property developed through years of R&D and investment. Instead the government should seek to create value for the entire sector by creating a conducive business environment that is facilitative of all business models overall.

Compliance Monitoring: Please see our response in relation to Question No.4 above. Given the sheer diversity of business models and practices, it would be difficult and overly restrictive to develop a one-size-fits-all approach to compliance monitoring by developing a single technology solution. In order to permit innovation to its fullest extent, the government must refrain from interfering prescriptively in compliance and only intervene in clear cases of market-failure. The most effective mechanism to achieve

optimal compliance would be by permitting industry to evolve self-regulatory codes and certifications which provide users with comfort and confidence that their information would be safely preserved, protected, and processed in accordance with stated practices. In fact, the current regulatory framework – under the IT Rules – expressly recognises the role played by industry-led certification efforts as a method of effective compliance with the requirement to implement security practices and procedures.

Such a framework would be ideal as it drives compliance by harnessing market forces and incentivising good privacy practices which are transparent. In the presence of effective certification programs, privacy practices would be driven by competition - ensuring the best possible protection for user data. A technology-based compliance mechanism as suggested by the question would by adopting a straight-jacketed approach drive up compliance costs and erect barriers at a time when a key focus of the government is to improve the ease of doing business and facilitate innovative practices.

Question 8

What are the measures that should be considered in order to strengthen and preserve the safety and security of telecommunications infrastructure and the digital ecosystem as a whole?

Response:
At the outset, it must be noted that most constituents of the telecommunications ecosystem are covered by the extant framework which includes the IT Act, IT Rules, in addition to the respective licenses and circulars of the Department of Telecommunications of the Government of India. However, in light of rising cyber threat levels, there are a number of steps that the government can take to protect security and ensure best practices in relation to telecommunications infrastructure and the digital ecosystem as a whole.

At the outset, innovation in security must be encouraged. In this regard, only the joint efforts of the government and private sector can ensure a net rise in security levels across the sector. Facilitating innovation in cybersecurity and compliance including by encouraging research and self-regulatory and certifications schemes can improve cyber-security and –hygiene levels across the sector – with the added benefit of stimulating compliance and creating a new market in which Indian enterprises can compete globally.

The government must also aim to improve consistency across cybersecurity and related regulation across sectors by bringing them in line with international best practices. This includes on issues such as encouraging strong and end-to-end encryption by issuing a relevant notification/policy after conducting broad-based public-consultations taking into account current industry and international practices. The need is urgent especially in relation to the telecommunications sector where some stakeholders are required to use 40-bit encryption keys and where bulk encryption is prohibited for others. Bringing these in line with international standards would be a precondition to evolving a robust cybersecurity ecosystem befitting a critical sector.

Question 9

What are the key issues of data protection pertaining to the collection and use of data by various other stakeholders in the digital ecosystem, including content and application service providers, device

manufacturers, operating systems, browsers, etc? What mechanisms need to be put in place in order to address these issues?

Response:
The key issues of data protection pertaining to the various stakeholders remain the same across various parts of ecosystem and at various stages of the value chain. At present, they are all subject to the robust framework contained in the IT Act and Rules. As the issues remain, so do the policy objectives for a regulatory framework. Regardless of sector, the approach must manifest a balance of facilitating innovation, ease of doing business, while ensuring the reasonable privacy expectations of users are satisfied.

While regulator for the sector, it must be ensured that user choice and volition are respected to the maximum extent. At the end of the day, most online services based on data are offered to users on a voluntary basis. In other words, users can opt out of the service at any point and decline to continue making use of the service in question. This more so the case as given the low costs of market entry, competition levels are high and new entrants are constantly making their mark in the sector. As a result, any regulatory approach must respect these economic realities and aim to preserve the status quo which has facilitated innovation.

A technology and platform neutral data protection law being worked on by MEITY may provide the way forward,

Question 10

Is there a need for bringing about greater parity in the data protection norms applicable to TSPs and other communication service providers offering comparable services (such as Internet based voice and messaging services). What are the various options that may be considered in this regard?

Response:
No. There is no need to ensure parity as the internet-based services and TSP-services operate are completely different market segments with unique regulatory and economic concerns. Treating them on par would fail to recognise these crucial distinctions and result in inefficient regulation which over-regulate one while under- or inappropriately regulating the other. From a regulatory point of view, each operates on a different technological plane. TSPs operate on the basis of exclusive spectrum allotted to them while internet based services operate on the open internet – not on the basis of exclusivity of any resource but on the merits of their business models and value addition to the internet at large.

TSPs own exclusive infrastructure (whether spectrum or physical) and this forms the basis for modern telecommunications. It is unavoidable for users to not use or be affected by TSP practices – whether for phone calls, faxes, or internet – but the internet-based service segment operates purely on a choice and consent based platform. Users are free to use or not use any service available online. Given this distinctions, there is a case to be made that TSPs must be regulated more closely given their exclusivity over resources while internet-based services must be regulated only where there is clear evidence of market failure. This conclusion also extends to the data protection realm where at present both segments are regulated in the same manner under the framework of the IT Act and applicable Rules.

Given the innovation-led and nascent stage of the internet-based service economy in India, the government must be doubly careful so as to ensure that innovative forces and business models are proposed. Despite being a recent phenomenon, internet based services have contributed more than USD 20 billion to India's GDP in 2015-16 and this share is only projected to increase. Till the sector reaches its equilibrium, and in the absence of any market failure, there is no rationale which may justify policy intervention in the sector generally – much less, to bring the same into parity with the TSP segment.

Question 11

What should be the legitimate exceptions to the data protection requirements imposed on TSPs and other providers in the digital ecosystem and how should these be designed? In particular, what are the checks and balances that need to be considered in the context of lawful surveillance and law enforcement requirements?

Response:
Legitimate exceptions to the Indian data protection should track international best practices. A failure to do so would lead to a regulatory arbitrage with entities preferring a jurisdiction with more certainty and less exceptions to protection. In line with international trends, exceptions must generally relate to compelling public interests such as national security and safety and must manifest in the form of a requirement to comply with legal requests issued in pursuance to the relevant due process requirements. At the same time, as discussed in responses above, certain forms of data such as anonymised data must be subject to lower levels of compliance requirements.

Checks and balances in relation to lawful surveillance and law enforcement mechanisms must come about through the government encouraging – rather than imposing – the deployment of robust cybersecurity norms and practices by private sector. The government must not seek to limit or cap the strength of encryption techniques or technologies and, as discussed above, must instead look to emphasise self-regulatory mechanisms as currently recognised within the IT Act framework and Rules. Examples of techniques that may be encouraged include end-to-end encryption, and the issuance of an encryption policy under the IT Act which – instead of prescribing limits on encryption – prescribes certain minimum standards. This would lead to strong encryption and security being incentivised and driven by market forces.

Question 12

What are the measures that can be considered in order to address the potential issues arising from cross border flow of information and jurisdictional challenges in the digital ecosystem?

Responses:
At the outset, it is important to understand the role played by cross border data flows in the modern digital economy. Not only do they drive innovation and development, but are a key characteristic of the connected world today. Any measure aimed at disrupting such flows would lead an economy or region being cut off from the global digital value chain, harming innovation, and losing out to other jurisdictions. In addition, consumer interests would be harmed by a decrease in choice, and lower access speeds. This would especially be deleterious for a growing economy like India. As such there is presently no policy or regulatory rationale to justify an intervention in the form of any measure such as localisation or geo-blocking which affects global cross-border data flows.

Challenges (if any) posed by cross border data flows are far outweighed by the benefits they bring to an economy or region. For instance, the Indian outsourcing industry is a key product of the free flow of information and communications across borders. Erecting national barriers online would also deprive the fledgling start-up economy of foreign customer bases and damage India's reputation as a stable investment destination.

Jurisdictional challenges are yet a recent phenomenon and a by-product of the evolving digital ecosystem. The most robust way to address them is by allowing international and governmental consensus to build through cooperative mechanisms. A number of countries have entered into information sharing and cybersecurity agreements which cover these aspects. As global consensus on the way forward builds, any attempt to regulate data flows would only result in disproportionate harm to stakeholders while cutting off India from the global digital economy.