Sangeet Sindan
(Legal Counsel)
Avocat De Confiance
(Sole Proprietorship)

Date: November 6, 2017

To,
Shri Bharat Gupta,
TRAI,
Phone: +91-11-23220209
Email:bharatgupta.trai@gmail.com

Sub: Comments on the consultation paper on privacy, security and ownership of data.

Ref: Consultation Paper on "Privacy, Security, and Ownership of the Data in Telecom Sector", dated August 9, 2017 ("Consultation Paper").

Dear Sir/Madam:

At the outset, I appreciate and welcome the Consultation Paper on the issues of "Privacy, Security and Ownership of the Data in Telecom Sector" issued by Telecom Regulatory Authority of India ("TRAI"). I am thankful to TRAI inviting all stakeholders to provide comments on the issues raised in the Consultation Paper. I submit my comments based on my work experience in the field of legal advisory for information technology companies and research conducted with regard to various issues mentioned in the Consultation Paper.

Data (a non-natural, economic and productive factor) is one of the key resources for various stakeholders in the Information Technology and Telecom sector; hence, ownership, control, management, and sharing of data etc. are significant and critical area of concern to delved into. Creation of regulated eco-system of data sharing, control and security will ensure: (i) fair and appropriate use of personal data of users ensuring customer security and privacy, (ii) seamless and optimal utilization of such economic resource across the industry for further advancement and innovation of IT services.

My comments, key ideas and points to the issues has set forth in line in the Annexure A attached hereto.

I would be glad to discuss these important issues further.

Yours faithfully,

S.Sindan

Sangeet
Legal Counsel
Avocat De Confiance

Email: sangeetsindan@gmail.com

ANNEXURE A

Introduction

The current legal framework of data protection is enshrined under the various laws and regulations of India:

1) The Section 43A of the Information Technology Act, 2000 ("ITA") and the Information Technology (Reasonable security practices, procedures and sensitive personal data or information) Rules, 2011 ("Data Protection Rules") which are applicable to all body corporates, including TSPs and "intermediary" that come under the ambit of Section 2(1)(w) of the ITA. In the current landscape of information technology industry, the term "intermediary" includes a gamut of IT enabled service providers engaged in the business of: (i) data conversion, data mining, data entry, data digitization, data processing etc. (ii) medical transcription, (iii) hosting service provider (sharing or managed), (iv) application service providers, (v) internet / web based e-commerce or online market place, (vi) smart card customization service, (vii) search engines, (viii) social media websites, and (ix) payment gateway and e-wallet service providers etc.;

2) The directives of Telecom Regulatory Authority of India ("TRAI") titled as "direction regarding confidentiality of information of subscribers and privacy of communications", dated February 26, 2010 issued to Cellular Mobile Telephone Service Providers and Unified Access Service Providers ("TRAI Guideline");

3) Rule 12 (i) and (ii) read with the Rule 11 (i) Insurance Regulatory and Development Authority of India (Outsourcing of Activities by Indian Insurers) Regulations, 2017 indirectly casts an obligation on the outsourcing service providers to implement such security policies, procedures and controls that enables insurance companies to protect and ensure confidentiality of information of the policy holders. Said that such ITES companies providing services as outsourcing service providers are bound to comply with the said rules through the outsourcing agreements; and

4) Paragraph 5.5 (Outsourcing Agreement) of the Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by banks, dated November 3, 2006 issued by the Reserve Bank of India ("RBI"), stipulates about imposing obligations on the outsourcing service providers rendering services to banks to ensure customer's data security and confidentiality, and liability in case of breach. Thus, an ITES company providing financial technological services to banks must adhere to such guideline.

The observations and comments for a stronger and coherent legal framework for data protection and privacy of an individual are based on my work of legal advisory over the past 7 years and consider the relevant research that I have conducted in relation to the legal and regulatory framework of European Union. My observations and comments not only touches the issues of data privacy in telecom sector but also covers some general principles that may be applicable to some information technology enabled service providers which are depending on telecom resources.

Please find my comments and observations as follow in turn.

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?*

   Comment:

   1) Limited Scope of Applicability of Section 72A and 45 r/w 43A of the ITA on Outsourcing Service Providers: It is pertinent to note that Section 72A of the ITA is applicable if the following key criteria is, *inter alia*, met, namely:

      i) Confidential Information should be disclosed knowingly and intentionally causing wrongful loss or wrongful gain;

      ii) There should be a contract between the service provider and the customer providing information to such service provider; and

      iii) The information has been disclosed without the consent of the information provider.

      Please note that there are various ITES companies (such as call centers, application service providers, data center, software as service providers etc.) which are also registered under "Other Service Provider" category. Such ITES companies provide services to different industries such as insurance, banking, telecom etc. These companies may not fall under the ambit of Section 72A of the ITA since above criteria may be missing. Typically, outsourcing ITES companies do not have any direct agreement with the information provider i.e. customers or users, and it is very difficult to prove that there was knowingly and intentional disclosure of personal information. However, such outsourcing service providers may be penalized by way of compensation under Section 45 r/w Section 43A of the ITA if there is a compromise in confidentiality of sensitive personal information of the provider causing wrongful gain or wrongful loss to any other person. In light of the foregoing, it can be construed that mere breach of confidentiality or ignorance of implementing the optimum level of information security practices and procedure is not sufficient to attract the provisions of Section 72A and 45 r/w 43A of the ITA.

   2) Narrow list of Sensitive Personal Information: in terms of Rule 3 of the Data Protection Rules read with explanation (iii) of Section 43A of the ITA, "sensitive personal data or information" includes: (i) password, (ii) financial information such as bank account or credit card or debit card, or other payment instrument details, (iii) physical, physiological and mental health condition, (iv) sexual orientation, (v) medical records and history, (vi) biometric information, (vii) any detail relating to the foregoing items as provided to body corporate for providing service; and (viii) any of the information received with respect to the foregoing by body corporate for processing, stored or processed under lawful contract or otherwise. The scope of definition of the sensitive personal data is narrow in comparison to the definition of "special category of personal information" stipulated under Article 9(1) of the "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016" which ("General

Data Protection Regulation") which covers the following categories of sensitive personal information in Article 9 and 10 of the said regulation, namely:

Article 9: processing of special categories of personal data

1. *Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of the genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.*

   …….

   Article 10: processing of personal data relating to criminal convictions and offences

   Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorized by Union or Members State law providing for appropriate safeguards for the rights and freedoms of the data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority."

   In light of the above, it can be construed that GDPR consists a more wider scope of sensitive personal data including: (i) special categories of personal data such as racial or ethnic origin, political opinion, religious or philosophical belief, membership of particular trade union, genetic and biometric data, medical details, sex life or sex orientation, and (ii) record of criminal conviction and offences.

3) Lack of Constructive Notice and informed consent: there are many Indian companies such as e-commerce, mobile application providers, smart phone manufacturer, social media etc. which come under the scanner of ITA and Data Protection Rules. In terms of Rule 4 of the Data Protection Rules such companies must publish a privacy policy on its website and also take a consent for gathering the sensitive personal data of the users; however, in many cases such requirements are not fulfilled completely and blatantly violated. The terms of use and privacy policy are not published on the conspicuous place of the website, hence violating the principal of constructive notice and there is no *consensus ad idem* between the user and the service provider. This essentially means, a user or consumer is not aware about the value, scale of use of his or her sensitive personal data or personal data.

   Further, it is pertinent to note that the consent of the users or consumers are not free rather it is conditional under the Data Protection Rules. In terms of Rule 5 (7) of the Data Protection Rules a body corporate may not provide the services or goods, or may discontinue with provisioning of services or providing goods if a user or consumer does not provide consent for collection of sensitive personal information or withdraw his/her consent later. For ease of reference, Rule 5(7) of the Data Protection Rules has been reproduced as follow:

"5. Collection of information. —

(7) Body corporate or any person on its behalf shall, prior to the collection of information including sensitive personal data or information, provide an option to the provider of the information to not to provide the data or information sought to be collected. The provider of information shall, at any time while availing the services or otherwise, also have an option to withdraw its consent given earlier to the body corporate. Such withdrawal of the consent shall be sent in writing to the body corporate. In the case of provider of information not providing or later on withdrawing his consent, the body corporate shall have the option not to provide goods or services for which the said information was sought."

In contrast to the laws of data privacy of other jurisdiction the condition of consent of Indian Data Protection Rules is not fair and equitable. Section 14(2) of the Personal Data Protection Act 2012(No. 26 of 2012)[1] of Republic of Singapore ("Singapore Data Protection Law") stipulates that providing services or product should not be a condition for procuring the consent of data provider, moreover, consent procured through false or misleading information will be void; for ease of reference the relevant provision of Section 14(2) of the Singapore Data Protection Law has been quoted as follow:

"14. (2) An organisation shall not —

(a) as a condition of providing a product or service, require an individual to consent to the collection, use or disclosure of personal data about the individual beyond what is reasonable to provide the product or service to that individual; or

(b) obtain or attempt to obtain consent for collecting, using or disclosing personal data by providing false or misleading information with respect to the collection, use or disclosure of the personal data, or using deceptive or misleading practices."

The Article 4(11) of the GDPR defines the consent as follow:

"'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;"

In light of the above, it can be construed that the consent of a consumer must be free and specific, and the privacy policy should be unambiguous; moreover, the consent must be taken through clear affirmative action of the data provider.

4) Absence of Supervisory Authority: though a few companies have published the privacy policy on its website, however, it is wanting of the compliance of a certain provisions of Rule 4 (1)

---

[1]*Personal Data Protection Act 2012 (No. 26 of 2012)* (*last accessed on October 21, 2017)* http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3Aea8b8b45-51b8-48cf-83bf-81d01478e50b%20Depth%3A0%20Status%3Ainforce;rec=0;whole=yes

of the Data Protection Rules, which mentions that the privacy policy shall provide for, *inter alia*:

i) Clear and easily accessible statements of its practices and policies*;*

ii) Type of personal or sensitive personal data mentioned under the Rule 3 of the Data Protection Rules;

iii) Reasonable security practices and procedures as provided under Rule 8. The said rule stipulates for implementing one of the standards of reasonable security practices i.e. international Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques - Information Security Management System - Requirements".

In terms of Rule 8(4) of the Data Protection Rules, a company falling under the ambit of Section 43A of the ITA must get audited of its reasonable security practices and procedures with regard to the data; however, the actual implementation of privacy policy in terms of said rule is unchecked since there is no supervisory authority to investigate the compliance level and implementation. Hence, the enforcement of data privacy law must be backed by a strong supervisory or enforcement authority.

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?*

Comment:

Rapid advancement of technology may also bring challenges to data protection and privacy of individual- e.g. use of digital wallet or other mobile application for payment, digital locker, posting of personal information on various social media sites, deployment of cameras or security instruments at various places, smart mobile devices, and storage of person data of provider in cloud system where storage resources controlled by different operating systems to provide services etc.

Personal data has been defined in a coherent way by various jurisdiction. Article 4(1) of the GDPR defines personal data in more broader sense: *"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".*

Further, recital 30 of the GDPR stipulates: "*Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol*

addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."

In light of the above definition, the scope of personal data is very broad in GDPR which includes the following items as well:

(i) Information, either in solely or in combination with other information, can lead to identify a person in particular reference, such as name, number or online identifier.

(ii) It includes also the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(iii) Information includes online identifiers pertaining to electronic, computer and telecommunication devices, tools and protocols whereby a person can be identified.

However, in contrast the definition of personal data under the Data Protection Rules is narrow and has limited scope which is summarized as follow:

(i) The definition of personal data has been provided under the Data Protection Rules. The substantive act should define the personal data and sensitive personal data, rather than delegating the power to define the definition and the related rights.

(ii) The definition of personal data is only restricted to identification of a person, resultantly, excluding a wide variety of personal information which may be related to physical, physiological, genetic, mental, economic, cultural or social identity of a natural person.

(iii) The Data Protection Rules is only applicable to body-corporates thereby excluding various entities and organization from its scope. Such non-body-corporates may include society, trust, sole proprietorship, associations etc.

(iv) In the era of smart phones and mobile applications, various categories of information does not come under the ambit of Data Protection Rules. Such information includes media access control address, phone number, wireless network or mobile network, and International Mobile Equipment Identity ("IMEI"), location of a user (in case of location based services), cookies etc. It was reported by *Hindustan Times* that *One Plus may have been collecting user data without permission*[2], such data includes, phone number, wireless network, MAC address IMEI number etc.

Hence, it is advisable to adopt the standard definition of personal data provided under the GDPR

---

2 Kul Bhushan*, OnePlus may have been collecting user data without permission* (last accessed on October 22, 2017) <http://www.hindustantimes.com/tech/oneplus-may-have-been-collecting-user-data-without-permission/story-zrAcYkQgnzUa2kobYlj5oK.html>

Recognizing ownership guarantees authority and protection of rights of an owner; hence, a data subject (to whom personal data relates to) should be recognized as the owner of the personal data; however, such ownership should not be absolute as well. The data subject should have the right to give consent before sharing of his/her personal data for commercial purpose; the said practice would provide the data subject a fair chance either to object or provider consent for sharing their personnel data outside the country. Hence, it would fulfill the requirement of second principle i.e. "choice and consent" mentioned in the Planning Commission report on establishing a National Level Privacy Principles. Also, following points should be considered to confer upon more capabilities and authority to a data subject, namely: (i) the right of access, (ii) the right to rectification, (iii) the right to delete, (iv) the right to restrict processing, (v) the right to data portability, (vi) the right to object (vii) right not to be traced unlawfully based on the personal data, and (viii) the right not to be subject to a decision based solely on automated processing.

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.*

Comment:

Data Controller has a significant roles and responsibilities in a comprehensive system of privacy laws. In terms of extant laws on data protection Data Controller, *per se*, has not been defined. The substantive laws should provide a definition of Data Controller and its rights and responsibilities which are outlined as follow:

(i) Data Controller must procure an explicit consent from the data subject before collecting the personal data and transferring such data;

(ii) A fair and legitimate processing of personal data must be ensured; failing to comply the same the Data Controller should be directly held responsible;

(iii) Data Controller should specifically appoint a data officer ensuring compliances under the laws and addressing the complaint of a data subject;

(iv) In case Data Controller outsource the function of processing of personal data then it must have full power to check and do a periodic audit of the outsourcing company. This practice will ensure that the Data Controller is primarily responsible for correct and fair use personal data during processing;

(v) Data Controller must provide access to the data subject to update, correct or delete non-relevant data from the system;

(vi) Sending a notice of breach and compromise in data confidentiality to respective data subject; such act would provide an opportunity to data subject to take appropriate action;

(vii) The data retention policy must be specifically mentioned in the user agreement and the period of data retention;

(viii) Standard minimum terms to be included in the data sharing agreement of the Data Controllers; and

(ix) Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data[3].

The ITA and Data Protection Rules do not provide any supervisory and government administrative body regulating and monitoring Data Controllers in India. In majority of the jurisdiction having a comprehensive system of data protection laws a data commissioner or equivalent administrative and supervisory body has been conferred upon with power to supervise, monitor and control data controller.

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?*

Comment:

Yes, a technology enabled architecture is very useful and worthy to audit the use of personal data. Certain software tools may help to understand and identify the personal data that can be used for processing. It may also help for data profiling whereby following things can be analyzed: (i) how the personal data is displayed, (ii) relationship of data residing in two systems, (iii) data mapping, (iv) identifying security loopholes or flaws in the operating systems and hosting servers where data is stored. Qualifications observed in audit shall not only help the companies to elevate the security level but also shall help the government as to new security risks, breach and cyber-attack and measures to be taken. Demographic dividend is boon for India and by capacity building, skill development and training a capable workforce of auditors can be nurtured. Such capacity building can be achieved through following ways:

(i) Certification program or diploma program that can be imparted through government institutions or through public private partnership establishments.

(ii) By conducting a workshop in collaboration with the industrial and regulatory stakeholders.

(iii) Promoting a separate degree or master course in the field of cyber-security or vocational training program.

---

[3]Data Sharing Code of Practice, Annexure 1-the Data Protection Principles (last accessed on October 26, 2017) https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf).

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?*

   Comment:

   Privacy and protection of data or personal information is a fundamental right of a data subject, hence, obligations and compliances mandated under any data protection is equal across all industry; however, it is pertinent to note that based on the nature of business or services the risk of data protection, and accountability and responsibility of data protection may vary e.g. in case of retail ecommerce industry the collection of information is only restricted to phone number and name whereas in case of healthcare or financial services the risk of privacy is very high. Further, large companies are capable of adapting with the compliance of new laws or a paradigm shift in the laws relating to data protection, however, small and medium enterprise or startups may have to face the heat and burn of extra burden of expenses of compliances. In backdrop of the foregoing, it is better to espouse and create a comprehensive, rational and industry friendly data protection laws balancing the conducive environment of compliance and effective protection of data or information of data subjective without any compromise. Following measure can be considered in the said regard, namely:

   (i) The scope and definition of data controller, data processor and data subject must be lucidly and clearly defined in the applicable laws;

   (ii) *Lex spectat naturae ordinem* - the law regards the order of nature; said that depending on the nature of risk and capacity to control the purpose, process and use of data, the responsibility and accountability of service providers (whether data controller or data processor) should be determined e.g. law should mandate a shared responsibility among the different service provider. In case of social media mobile application there are broadly two layers involved, the first is user interface of the mobile application and the second layer is the hosting provider which hosts the backend operating platform of the mobile application. In that case mobile application provider is only liable for data integrity, data authentication, data encryption, server side encryption whereas the hosting provider is accountable and responsible for hosting, storage, backend network security and data location. The mobile application provider is required to disclose and mention the details of hosting provider location of data to be stored. Also, it should be responsibility of the hosting provider to provide options of location for storing of data.

   (i) In case of cross transfer of personal data outside India a prior approval of Indian supervisory authority should be compulsory.

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?*

Comment:

A data sandbox isolates certain data from a large pool of data, consequently, allow a data steward to access and experiment a small set of data in managed and controlled environment, therefore, data sandbox offers additional protection to personal data. This would especially bolster fin-tech or start-ups entities to experiment certain data and innovate new services in various fields such as peer-to-peer lending, microfinance, cryptocurrencies, crowdfunding, use of Blockchain technology, insurance etc. The platform of sandbox has advantages of better risk management, creation of new opportunities and innovation of technology, efficiency and protection of consumers. Testing a product or services in the environment of regulatory sandbox would provide opportunity to weigh the risk posed to the customer and benefits; if the risk outweighs the benefits of such products or services then the launch of the product will be discontinued.

A few of the jurisdictions such United Kingdom, Singapore, Malaysia, Australia, and UAE have introduced regulatory sandbox[4]. Following examples throws light on positive approach and experimentation by various countries relating to regulatory sandbox for a diverse range of sectors:

(i) Blockchain technology may be experimented to solve the problem of fake digital advertisements. Blockchain technology provides a digitized distributed ledger which records and adds the completed transaction in chronological order, thereby, the authenticity of a transaction can be identified and tracked. Further, the said technology can be also used for settlement of a transaction and smart contracts[5].

(ii) The Financial Regulatory Authority of United Kingdom ("FRI") issued a press release whereby it published the list of fin-tech firms that are allowed to begin with testing.

List of Firms Permitted by FRI for Testing[6]

Firm	**Description**
Billon	An e-money platform based on distributed ledger technology that facilitates the secure transfer and holding of funds using a phone based app.
Bit X	A cross-border money transfer service powered by digital currencies / block chain technology.

4 Vikas Dhoot, *Regulators Shouldn't restrain innovations*, (last accessed on October 28, 2017) http://www.thehindu.com/todays-paper/tp-business/regulators-shouldnt-restrain-innovation/article19382071.ece
5 Regulatory Sandbox Making India a Global Fintech Hub, pp. 14 (last access on November 5, 2017) https://www2.deloitte.com/content/dam/Deloitte/in/Documents/technology-media-telecommunications/in-tmt-fintech-regulatory-sandbox-web.pdf
6 *Financial Conduct Authority unveils successful sandbox firms on the second anniversary of Project Innovate*, dated November 11, 2016, (last accessed on November 6, 2017) https://www.fca.org.uk/print/news/press-releases/financial-conduct-authority-unveils-successful-sandbox-firms-second-anniversary

Blink Innovation Limited	An insurance product with an automated claims process, which allows travelers to instantly book a new ticket on their mobile device in the event of a flight cancellation.
Bud	An online platform and app which allows users to manage their financial products, with personalized insights, on a single dashboard. Bud's marketplace introduces relevant services which users can interact with through API integrations.
Citizens Advice	A semi-automated advice tool which allows debt advisers and clients to compare the key features of available debt solutions.
Epiphyte	A payments service provider that aims to provide cross-border payments using block chain technology.
Gov coin Limited	A technology provider that has partnered with the Department for Work and Pensions (DWP) to determine the feasibility of making emergency payments using means other than cash or the Faster Payments Scheme. The payments platform will use block chain to allow the DWP to credit value to a mobile device to transfer the value directly to a third party.
HSBC	An app developed in partnership with Pariti Technologies, a Fin Tech start-up, to help customers better manage their finances.
Issufy	A web-based software platform that streamlines the overall Initial Public Offering (IPO) distribution process for investors, issuing companies and their advisors.
Lloyds Banking Group	An approach that aims to improve the experience for branch customers which is aligned with the online and over the phone experience.
Next day Property Limited	An internet-based property company that will provide an interest free loan for a guaranteed amount to customers if they are unable to sell their property within 90 days.
Nivaura	A platform that uses automation and block chain for issuance and lifecycle management of private placement securities.
Otonomos	A platform that represents private companies' shares electronically on the block chain, enabling them to manage shareholdings, conduct book building online and facilitate transfers.

Oval	An app which helps users to build up savings by putting aside small amounts of money. These savings can then be used to pay off existing loans early. Oval will be working with Oakam, a consumer credit firm and a number of their customers during the test period.
SETL	A smart-card enabled retail payment system based on their Open CSD distributed ledger.
Tradle	An app and web-based service that creates personal or commercial identity and verifiable documents on a distributed ledger. In partnership with Aviva they will provide a system for automated customer authentication.
Tramonex	An e-money platform based on distributed ledger technology that facilitates the use of "smart contracts" to transfer donations to a charity.
Swave	A micro savings app that provides an across-account view; enables a round-up service every time a user spends money and calculates an affordable savings amount based on the user's spending behaviour.

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?*

   Comment:

   Effective monitoring and supervision of digital ecosystem requires an agile approach from the government authorities or regulators; it would help to keep pace with the technological advancement as well as protection of large stakeholder participating in the digital ecosystem. Following points can be considered for setting up a technological solution for monitoring and supervising the digital ecosystem for compliance:

   (i) Mandatory registration of Application Program Interface ("API") used for transaction related services such as transmission of sensitive personal information i.e. credit card, bank details etc. and user authentication. This would help the government agencies to test the security level of the APIs involved in financial transactions and to identify the key loopholes in the technology used. Said that a mandatory classification of APIs is required such Product API, Marketing and Sale API, Servicing API and Transactions API, and other Information API. Further, a statutory obligation should be casted on the payment gateway industries for adopting the latest Payment Card Industry Data Security Standard.

   (ii) Artificial intelligence can be used to monitor the trend of illegal transaction and pattern thereof. This can be achieved by using the machine learning for data mining algorithm.

(iii) Technological tools to block the APIs used for transaction services that are not duly registered with the government authorities.

The key attribute of such regulatory technology should: (i) real time reporting to the government authorities of any breach and violation of compliances, (ii) to provide a visibility and effective control to the government authorities, (iii) real time assessment of degree of risk of any threat and loopholes in compliances, (iv) prior signal and warning to the business entities which are not complying with the guideline or directions of the regulatory body or government authorities (i) effective and efficient method of receiving the complaints from the user and resolving the issues on timely manner.

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?*

Comment:

One can observe the convergence of telecommunication technology – the unified communication technology has integrated all communication service such as instant chatting, voice over IP, audio, web and video conferencing etc.; the packet switching technology and PSTN both have been converged to provide the telecommunication services.

The evolutionary advancement of technology in telecommunication infrastructure has also brought certain safety issues and threat to telecom infrastructure. DDoS is one of the critical threats hitting harder to the telecom infrastructure; it overwhelms the traffic route from multiple sources resulting either in slower telecom services or absolutely stopping the telecom services. The regulatory body should direct the providers of telecom infrastructure to keep the pace with latest technology and installing the same to protect the network e.g. (i) automated threat detection intelligence which can identify geo-location of data and know sources of threats (such as known malwares) to mitigate the risk (ii) implementing hybrid or multilayer of defense to mitigate the risk of DDoS (iii) deploying such tools and software which prohibits Data exfiltration. It is pertinent to note that on Other Services Providers (such as data center providers, hosting providers etc.) the terms and conditions of United License is not applicable, said that the following provision is not applicable on them:

"*The LICENSEE shall induct only those network elements into its telecom network, which have been got tested as per relevant contemporary Indian or International Security Standards e.g. IT and IT related elements against ISO/IEC 15408 standards, for Information Security Management System against ISO 27000 series Standards, Telecom and Telecom related elements against 3GPP security standards, 3GPP2 security standards etc. The certification shall be got done only from authorized and certified agencies/ labs in India or as may be specified by the Licensor. The copies of test results and test certificates shall be kept by the LICENSEE for a period of 10 years from the date of procurement of equipment."*

The above provision must also be included in the terms and conditions of the Other Service Provider compelling to deploy such equipment and technology commensuration to the extant need of cyber security.

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?*

Comment:

There are various participants and players in digital ecosystem and each one of them collects the personal data relating to their services with or without knowledge of a consumer. In case of smart mobile phones, a manufacturer may collect various personal information of consumer such as phone number, wireless network, MAC address IMEI number etc. Based on the nature of services to be provided by a mobile application, following information of a data subject is collected:

(i) Name, number, address or location (i.e. GPS localization recordings), phone number, health conditions and history (if required).

(ii) Access to the devices mobile such as camera and microphone devices.

(iii) Bank account and payment card details such as credit or debit card.

(iv) Cookies and browsing history which are collected during surfing or web browsing.

(v) Deleted message or information which can be retrieved with advanced technology.

(vi) Wireless connection details, type of connection, IP address and application usage etc.

(vii) Commutation and travelling details.

(viii) Saved password, personal files and folders, calendar data and contract data.

(ix) Details relating to Gyroscope and accelerometer.

Considering the exponential use of smart phones and tablets following points should be considered and mandated to the players of digital eco-system:

(i) Only such information and data should be collected by the mobile application developers that is strictly necessary to render the lawful functionality as identified for the mobile application. Hence, subject to scope of services data collection should be minimized commensuration to the purpose.

(ii) Express statement by the service providers as to nature and types of data collected by them.

(iii) Details of data protection officer and mechanism of grievance resolution.

(iv) The method of accessing the personal data and to ensure the accuracy of the same.

(v) Express statement about the purpose of collection and usage of personal data. In case of change of the purpose, the same must be expressly and unambiguously communicated to the data subject within reasonable time period and prior to enforce so that the consent from the data subject can be procured.

(vi) Method of withdrawing the consent for processing of the personal data.

(vii) Justifiable and reasonable method of obtaining the consent of the user or data subject before installing the personal data.

(viii) Clear system of identifying whether the communication through the equipment, or mobile application is done in encrypted form. In certain web browsers encryption level can be identified.

(ix) Choice or option in selecting needed and unneeded functionality e.g. in social media application if one wants to disable the location tracking function, however, wishes to keep on other function then such option should be available.

(x) System or method to check that the personal information stored in the mobile devices are encrypted.

(xi) Period of retention of personal information and the method of destruction and confirmation post deletion.

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?*

Comment:

Yes, it is high time that data protection norms should be applicable equally applicable to the TSPs and other communication service providers who are providing the services based on the VoIP/internet telephony or web-based/interest-based messengers; regardless of the technology providers of internet telephony or web-based messengers do the function of telecommunication. Thus, if the technology is kept aside, the services of application providing internet telephony or web-based messaging and the services of internet or telecom service provider are similar in nature. Internet based voice and messaging services are technological substitute of voice and messaging services provided by the TSPs.

It is pertinent to note that: (i) the provider of internet telephony or web-based messaging may not fall under the category of Other Service Providers, consequently, the terms and conditions of Unified License Agreement or Revised “Terms and Conditions - Other Service Provider (OSP) Category” may not be applicable, (ii) the obligations of confidentiality of customer information, customer protection regulation, privacy of communication and lawful monitoring and interception may not be applicable and enforceable on the providers of internet telephony or web-based massaging; thus, skipping the regulatory guidelines or directions. Hence, it is high time to bring the providers of internet telephony or web-based messaging under the

regulatory regime by imposing a fair and reasonable directions. Following measures can be considered in this regard:

1. TRAI should be conferred upon the power to for registration of service providers providing the services of internet telephony or VoIP on B2B or B2C basis.
2. Imposing guidelines, regulations or directions on the said providers with respect to standards of quality, security, data retention, and compliances.
3. The network-architecture of VoIP includes various software cum hardware elements including Session Border Controller, Application Server, Network Address Translator Servers, Media Gateway, and Media Servers. The architecture should be arranged in such a way the key elements should remain and localized in India. This would help the law enforcement agencies for lawful interception and tracking of call or message in accordance with the laws.

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?*

Comment:

The telecom services broadly include internet services and telephone or mobile services; in either category, a TSP has a very wide scope of collecting, storing or sharing the personal information or data of a data subject. Every bit of data, information, text etc. flows through the telecom resources of a Telecom Service Provider. Said that there is a significantly high risk of encroaching the right of privacy of an individual.

In the case of *Justice K.S. Puttaswamy vs Union of India*[7], the Supreme Court of India has given a verdict that right to privacy is a fundamental right. Said that a legitimate expectation of benefit, relief or remedy to the data subject or provider must be established. In connection there to following points should be mandated to the TSPs: (i) the privacy policy and statement must be made a part to the consumer subscription form and option should be provided as to types of data which a consumer would like to share, (ii) telephone numbers, IP address and email must be kept confidential and must not be shared or transferred without express consent of a consumer; it has been observed that many TSP does not provide a privacy policy on the subscription form or application, rather a privacy policy lies on the website of the TSP, (iii) a data subject should have the right of privacy in relation to clickstream data which is a digital footprint during web browsing, a clickstream data is used to track online experience and to monitor the behavior of a consumer, (iv) the privacy policy or statement must specifically state the period of retention of personal data of a data subject (v) appointing data officer for addressing the queries, complaint and issues of a consumer raised in regard to the personal

[7] Writ Petition (Civil) No. 494 of 2012

data or information, (vi) developing a security system or check to mitigate the threat of SIM cloning.

Surveillance under the judicial supervision is a lawful and judicious supervision of any interception of telecom network or equipment. If the law enforcement agencies required to hack certain system or equipment then should procure an appropriate order from the court of law. The technologies, tools and techniques of hacking used by law enforcement agencies must commensurate to the gravity of crime and the quantum of evidence required in the court of law to prove an offence in the court of law. Said that it would better to conduct any hacking methodology in supervision of judicial officer who is capable of recording only such information required for case.

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?*

Comment:

In globalized world, especially in information technology sector and era of cloud computing, cross border flow of data and information cannot be prohibited, however, at the same time the inherent risk cannot be ignored as well. Following are the key potential risk to be considered and pore over:

(i) Transfer and storing the personal data to enemy countries or the countries having hostile relationship. If personal data resides in such country then it may cause threat to security of personal data of Indian residents.

(ii) Dearth of comprehensive legal system and mechanism to ensure that the outsourcee company has adequate and sufficient level of protection of personal data in the country outside India.

(iii) If there is a violation of data confidentiality breach then whether the other jurisdiction has framework of enforcement cooperation.

(iv) There may the case that the laws of other jurisdiction arbitrarily compel and mandates to disclose the personal data of an individual that may result into undermining the fundamental rights of data subject;

(v) Hosting of personal data of Indians in Indian territory i.e. data localization. A few of the jurisdiction e.g. Russia has mandated for data localization. Personal sensitive data or information must not be transferred cross border.

(vi) Specific conditions to be laid down and dictated to data controller in India before transferring personal data in relation to outsourcing of work; especially in case of banking, insurance and fin-tech companies.