Reliance Communications Limited's Response to the Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector

Executive Summary

A. **The data protection requirements currently applicable to all the players in the eco-system in India are not sufficient to protect the interests of telecom subscribers as the measures for data protection are only obligated on licensed network operators in the telecom eco-system and not on the device manufacturers, application(s) providers and OTT service providers.**

B. **For effective protection of data of the users' of the handsets, there is a need to enforce stricter compliance for protection of users' data collected by the handset / Tab / Laptop manufacturers, especially, when the user has consented only to give access to that information.**

C. **In light of recent advances in technology, there is a need to enlarge the list of information relating to an individual as defined at para 3 of the IT Rules 2011 and should include (a) Online Activity, (b) Information stored in personal devices and (c) Information obtained from personal use M2M devices like health devices, connected cars, e-meters, etc as personal information.**

D. **User's explicit consent should be taken before sharing his / her personal data for commercial purposes.**

E. **There is an urgent need to implement Rules 5 and 6 of the IT Rules 2011 for ensuring that due permission is taken of each user before accessing and sharing of his / her information for any use.**

F. **If any mobile app indulges in collection of personal data of the users they should be mandated to register themselves with TRAI and obligated to elucidate the reasons for which the app intends to collect the users' personal data. For ease and simplicity sake, this registration process should be made online.**

G. **The Data Controllers should have obligations, similar to TSPs, for protecting users personal data and should be permitted to collect data only after due consent from the user.**

H. **The Rights of Data Controller cannot supersede the Rights of an Individual over his / her Personal Data. However, exception to such Rights shall have to be made for LEAs in national interest only.**

I. **The Data Controller should be responsible for ensuring the security of the collected data and should be permitted to share data, preferably annonimised, for commercial purposes only after obtaining due consent from the user.**

J. **TRAI should impose suitable penalties on data controllers, similar to TSPs, for any breach of privacy of the user.**

K. **TRAI should be empowered to order blocking of content violating these norms.**

L. **For effective regulation and governance, local hosting of apps and their data bases should be mandatory.**

M. **It is most desirable to create technology enabled architecture to audit the use of personal data, and associated consent as it will provide sufficient visibility for the government or its authorized authority to prevent harm.**

N. **Annonimization of data set is an effective measure that must be taken before encouraging the creation of new data based businesses consistent with the overall framework of data protection.**

O. **Licensed operators too should be permitted to exploit their users data, in an annonimized form, for commercial purpose.**

P. **LEA requirements and usage of annonimized data can be considered as the legitimate exceptions to the data protection requirements imposed on TSPs and other providers in the digital ecosystem.**

Q. **Government or its authorized authority should not setup a data sandbox, which allows the regulated companies to create anonymized data sets which can be used for the development of newer services.**

R. **TRAI has recently launched a plethora of apps for speed testing, reporting of UCC, etc. A similar endeavour should be made by TRAI for setting up a technology solution that can assist it in monitoring the ecosystem for compliance.**

S. **With introduction of newer technologies such as Network Function Virtualization (NFV), virtual mobile networks become vulnerable to a number of security threats and are required to be addressed in the right earnest.**

T. **For ensuring uniformity of encryption policy at the national level there is a need to ensure that a single entity prescribes standardized encryption levels for attaining uniformity across services in India.**

U. **For addressing the jurisdictional challenges arising out of cross border flow of user's personal data and information, local hosting of users personal data, especially by the data collectors, should be mandated.**

V. **India should have maximum possible number of "Mutual Legal Assistance" agreements for getting information from data collector's setups hosted in cloud setups outside of India's territorial boundaries.**

Detailed Response

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?

Our Response

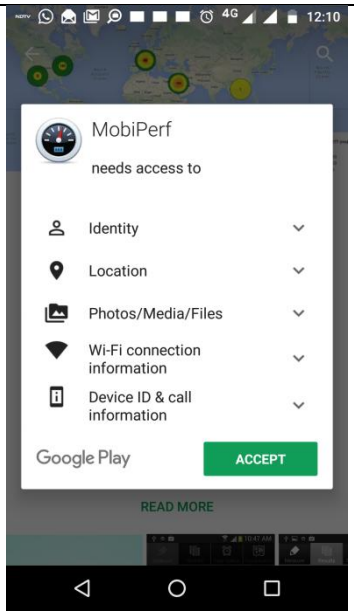
No, the data protection requirements currently applicable to all the players in the eco-system in India are not sufficient to protect the interests of telecom

subscribers as the measures for data protection are only obligated on licensed network operators in the telecom eco-system and not on the device manufacturers, application(s) providers and OTT service providers.

1. The telecom eco-system consists of the Devices (User handsets, Tabs, Laptops), Network elements (and supporting systems like billing, data storage, etc), Applications used by the users. Out of these components of the telecom eco-system, only the network providers are obligated to obtain a license from the govt and are held accountable for data protection requirements of their respective subscribers as part of the license conditions. The other two stakeholders in the telecom eco-system, viz the device manufacturers and the application providers are under no obligation for protection of their users' data.
2. **Device manufacturers.** Most of the devices available in Indian market come with preloaded, proprietary as well as general purpose applications. The user of the device is totally oblivious to the background activities that these apps perform which at times involves auto storing of data into the cloud spaces that have been created by the device manufacturers. It is a known fact that OS like Android undertake pseudo tracking of the users by tracking their handset itself. Android has the inbuilt settings for recording the users' activities over the internet and sharing this information with the advertises for targeted advertising. Though the feature can be disabled, but the default setting is enabled and the users are not notified about the same.
3. As per a news report[1], "Government fears Chinese smartphone makers stealing data, sends notice to 21 companies", by Ms Sneha Saha, published on 17 Aug 17 in the online magazine 'Indiatoday in Tech', the government has expressed concern about the likely-hood of hacking of users' data on their handsets. Therefore, **for effective protection of data of the users' of the handsets, there is a need to enforce stricter compliance for protection of users' data collected by the handset / Tab / Laptop manufacturers.**
4. **Application and OTT Service Providers.** Almost all apps, without exception, ask for access to a host of information from the user before permitting download of the app. In view of lack of any legal framework for sharing of information, obtained from a users' handset, which the user consents only to give access to the app and not to share it with a third party, the subscriber faces the challenge to either agree to the terms of the app provider and putting at risk his as well as others' privacy or is prevented from the use of the app only. E.g. It is difficult to understand as to why should a speed testing app or a network performance measuring app like 'MobiPerf' be accessing the users' personal information.

[1] http://indiatoday.intoday.in/technology/story/government-fears-chinese-smartphone-makers-stealing-data-sends-notice-to-21-companies-to-share-security-information/1/1027784.html

5. Though the user gives his consent for 'ACCESS' to the information on his device, but the apps 'SHARE' this information with the third parties, e.g. True Caller App shares individuals' mobile number with all users using True Caller app. **The IT act, clause 72 (reproduced below for ready reference), addresses sharing of information obtained without the consent of the owner of the information and not the scenario, where the owner of the information gives his consent for only accessing the information and not sharing it with the third parties.**



Why should MobiPerf, a network performance measuring app be asking access to all this information?

> "*72. Penalty for breach of confidentiality and privacy.*
>
> *Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book / register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both*."

6. In contrast the licensed operators are bound by their respective license conditions as well as the laws of the land such as the IT Act. **Therefore, there is indeed a need to address this issue of data protection from a user's handset when the user has consented only to give access to that information.**

<u>Our Recommendations</u>

7. In view of the foregoing, following are recommended,
   a. **The data protection requirements currently applicable to all the players in the eco-system in India are not sufficient to protect the interests of telecom subscribers as the measures for data protection are only obligated on licensed network operators in the telecom eco-system and not on the device manufacturers, application(s) providers and OTT service providers.**
   b. **For effective protection of data of the users' of the handsets, there is a need to enforce stricter compliance for protection of users' data collected by the handset / Tab / Laptop manufacturers.**
   c. **There is indeed a need to address the issue of data protection from a user's handset when the user has consented only to give access to that information.**

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?

Our Response

Yes, in light of recent advances in technology, changes are recommended to the definition of personal data as defined in IT Rules 2011.

Yes, the User's explicit consent should be taken before sharing his / her personal data for commercial purposes.

1. **Additions Required in the Definition of Personal Data.** A research on the internet reveals that since 2008, a new version of the 'Android' OS has been released every year as shown in the table below. A similar evolution cycle has been followed by numerous other popular applications.

Android Code Name	Version Number	Initial Release Date
(No codename)	1.0	September 23, 2008
(Internally known as "Petit Four")	1.1	February 9, 2009
Cupcake	1.5	April 27, 2009
Donut	1.6	September 15, 2009
Eclair	2.0 – 2.1	October 26, 2009
Froyo	2.2 – 2.2.3	May 20, 2010
Gingerbread	2.3 – 2.3.7	December 6, 2010
Honeycomb	3.0 – 3.2.6	February 22, 2011
Ice Cream Sandwich	4.0 – 4.0.4	October 18, 2011
Jelly Bean	4.1 – 4.3.1	July 9, 2012
KitKat	4.4 – 4.4.4	October 31, 2013
Lollipop	5.0 – 5.1.1	November 12, 2014
Marshmallow	6.0 – 6.0.1	October 5, 2015
Nougat	7.0 – 7.1.2	August 22, 2016
Oreo	8.0	August 21, 2017

Table 1 : Showing the evolution of Android Versions from its initial introduction in 2008

2. Given the pace of technological changes as well as the rate of introduction of new innovative applications, it is warranted that the IT rules too should match the pace of technological advancement to ensure their relevance in the current scenario of technological advancement.
3. The current IT Rules were published in 2011 and ever since no amendment has been issued by MeitY. Presently, para 3 of the IT Rules 2011 lists only the following items that are related to personal information.

> *"**Sensitive personal data or information.—** Sensitive personal data or information of a person means such personal information which consists of information relating to;—*

(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;

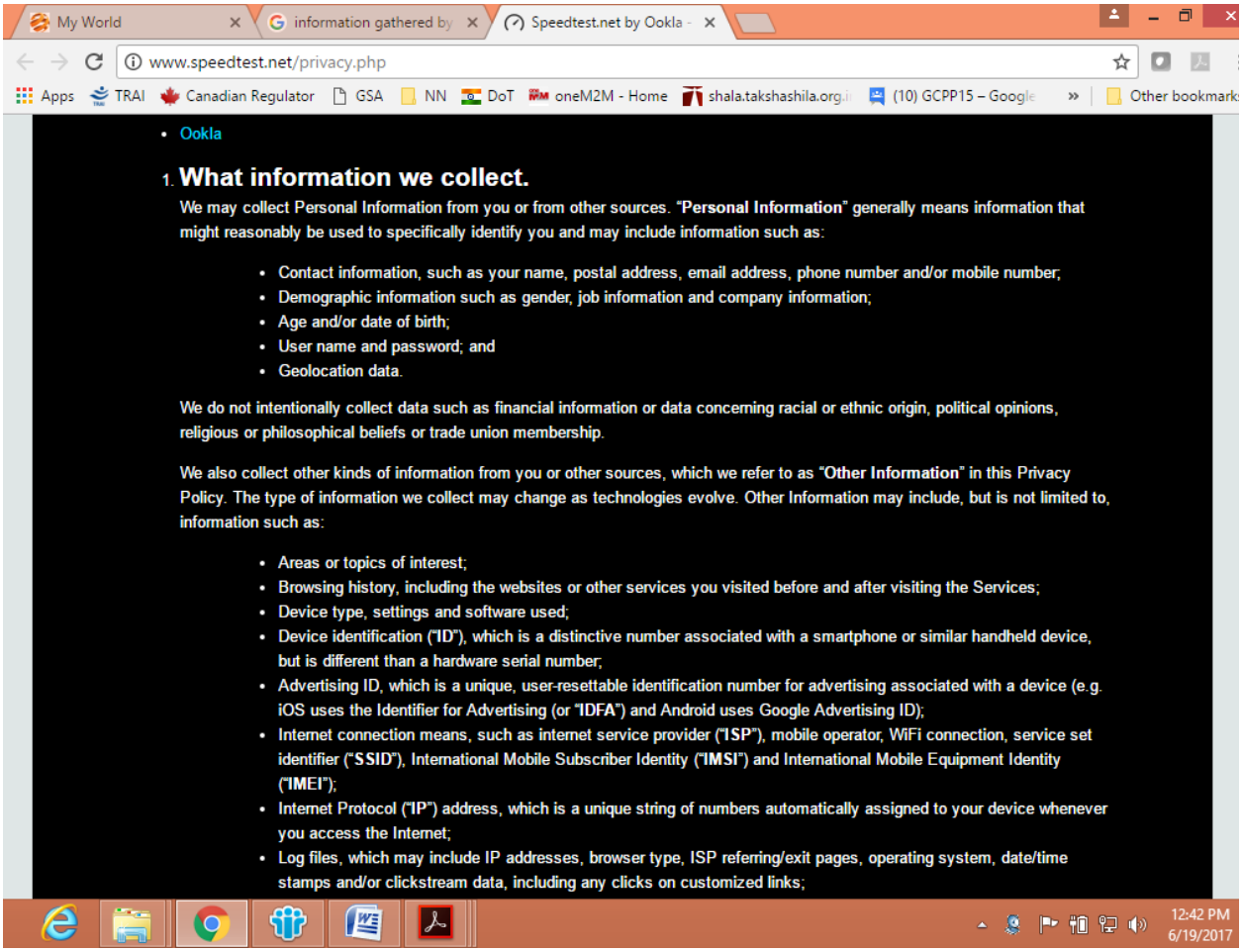
(vi) Biometric information;

(vii) any detail relating to the above clauses as provided to body corporate for providing service; and

(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules."

4. However, since 2011 there have been numerous technological changes, especially in the social networking and M2M services domain that enable collection of personal information about an individual. The information so generated has the ability to clearly identify an individual and hence **there is a need to enlarge the list of information relating to an individual as defined at para 3 of the IT Rules 2011. Following additional items are suggested to be included to the original list of information related to personal information.**
   a. Online Activity.
   b. Information stored in personal devices.
   c. Information obtained from personal use M2M devices like health devices, connected cars, e-meters, etc.
5. **Collection and Sharing of Personal Information for Commercial Purposes.** It is an open fact that the usage of any mobile app is subject to a user compulsorily agreeing to share his / her contact list and at times even the messaging list. Even if the functionality of the app has no relevance to the requirement of accessing the contact list, still the apps insist on its access and the user is forced to agree to the terms and conditions of the apps. E.g. Ookla, which is a data connection speed testing app forces its users to agree to sharing their contact details and other personal information as shown in the screen shot below. To give it a shroud of transparency, they openly declare the information that they are going to access but the point still remains that what is the requirement for a connectivity speed test app to gather this information? The TRAIs own data speed app, with similar functionality, does not impose such forced conditions on its users.



Screen Shot showing the declaration at Ookla website about the information that they collect from their users.

Source: http://www.speedtest.net/privacy.php

6. As can be seen from the screen shot above, the information being collected viz, postal address, email address, mobile number, gender, job information, age, date of birth, user name and even the password, geo-location are enough to uniquely identify an individual and hence can be classified as personally sensitive. The only way Ookla can make use of this information is by sharing the details of the subscriber's alongwith the device details with the online advertisers for targeted advertizing and hence monetizing it. The permission that Ookla takes is for accessing the data and not for sharing it. Additionally, the transparent declaration for the information that it is accessing, does not state the end use of this information.
7. Rule 5 and 6 of the IT Rules 2011 clearly define the mechanism, i.e. explicit consent of the person to whom the information is related to, to be adopted for collection and disclosure of the personal information. The rules clearly stipulate that,

   *"**Rule 5 (1) :** Body corporate or any person on its behalf shall obtain consent in writing through letter or Fax or email from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information.*

Rule 6 (1): *Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information"*

8. Despite the existence of rules that prohibit sharing of the personal information, even if obtained with due permission of the individual, the mobile apps have been violating these rules and utilizing the users' personal information for commercial gains by sharing this information for targeted advertizing. Hence, **there is an urgent need for strict enforcement of Rules 5 and 6 of the IT Rules 2011 for ensuring that due permission is taken from each user before accessing and sharing of his / her information for any use.**
9. **Measures to be considered for empowering the users to own and take control of his / her personal data.** TSPs and ISPs are the original collectors of a users' personal data for his / her identification. As signatories to the govts license permitting them operation of telecom networks in India, they are legally bound by the license conditions, one of which is to ensure the safety of users data and not share the same without the explicit consent of the user. Any unsolicited / illegal use of the subscribers' personal data, even the billing information, leads to penalization of the licensee. Such penalty imposition acts as deterrent and the licensees try to remain within the ambit of the law. The licensing regime has stood the test of the time and proved to be an efficient means for empowering the users in respect of ownership and control of their personal data. **Though licensing would be desired for exercising better control over the use of users' personal data, however, for the sake of providing an environment conducive for innovation, it is recommended that if any mobile app indulges in collection of personal data of the users they should be mandated to register themselves with TRAI. For ease and simplicity sake, this process for registration should be made online. While registering the app should be obligated to elucidate the reasons for which the app intends to collect the users' personal data.**

<u>Our Recommendations</u>

10. In view of the foregoing, following are recommended,
    a. **In light of recent advances in technology, there is a need to enlarge the list of information relating to an individual as defined at para 3 of the IT Rules 2011. Following additional items are suggested to be included to the original list of information related to personal information.**
        i. **Online Activity.**
        ii. **Information stored in personal devices.**
        iii. **Information obtained from personal use M2M devices like health devices, connected cars, e-meters, etc.**
    b. **User's explicit consent should be taken before sharing his / her personal data for commercial purposes.**

c. **There is an urgent need to implement Rules 5 and 6 of the IT Rules 2011 for ensuring that due permission is taken of each user before accessing and sharing of his / her information for any use.**

d. **If any mobile app indulges in collection of personal data of the users they should be mandated to register themselves with TRAI. For ease and simplicity sake, this registration process should be made online.**

e. **While registering the app should be obligated to elucidate the reasons for which the app intends to collect the users' personal data.**

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.

Our Response

The Data Controllers should have obligations, similar to TSPs, for protecting users personal data.

No, the Rights of Data Controller cannot supersede the Rights of an Individual over his / her Personal Data. However, exception to such Rights shall have to be made for LEAs in national interest only.

For regulating and governing the Data Controllers they should be asked to register themselves, through an online process, with TRAI.

1. **Rights and Responsibilities of the Data Controllers.**

   a. Collection of Data. Any form of communication requires an individual to be identified uniquely for the purpose of sending and receiving communications to other individuals, billing, subscription to customised services, etc. Therefore, a communication system provider has to collect an individual's personal details for creating a users' profile in the communication system. However, to prevent any misuse and to protect the privacy of the individual it is imperative to obligate the communication system provider / any other data collector to ensure the security of the collected data. Accordingly, following responsibilities should be entrusted to the data collectors,

      i. **The Data Collector should be permitted to collect data only after due consent from the user.**

      ii. **The Data Collector should be mandated to transparently communicate, to the user, the purpose for which users' personal data is being collected.**

      iii. **The Data Collector should be responsible for ensuring the security of the collected data.**

   b. Sharing of Data by the Data Collector for Commercial Purpose. The Hon'able Sc has recently ruled that privacy is a fundamental right. Therefore, any breach of privacy of an individual, attributed to the wilful sharing (Without consent) / leakage of the individuals' personal data, from the data collectors custody should be

construed as a violation of the fundamental right of that individual and dealt with under the IPC. However, **there can be situations where the user has given legitimate consent for sharing of his personal data as it is or in an annonimized form. In such cases, especially in annonimized form, the data controller should be permitted to share the data for commercial purposes.**

2. **Mechanism for Regulating and Governing the Data Controllers.** The mechanism for regulating and governing the Data Controllers should be similar to that of the TSPs wherein,
   a. Data Controllers should be mandated to register themselves with TRAI. For ease and simplicity sake, this registration process should be made online.
   b. TRAI should impose suitable penalties, similar to TSPs, for any breach of privacy of the user.
   c. TRAI should be empowered to order blocking of content violating these norms.
   d. For effective regulation and governance, local hosting of apps and their data bases should be mandatory.

Our Recommendations

3. **In view of the foregoing, our recommendations are as given below.**
   a. **The Data Controllers should have obligations, similar to TSPs, for protecting users personal data.**
   b. **The Rights of Data Controller cannot supersede the Rights of an Individual over his / her Personal Data. However, exception to such Rights shall have to be made for LEAs in national interest only.**
   c. **The Data Collector should be permitted to collect data only after due consent from the user.**
   d. **The Data Collector should be mandated to transparently communicate, to the user, the purpose for which users' personal data is being collected.**
   e. **The Data Collector should be responsible for ensuring the security of the collected data.**
   f. **The Data Collector should be permitted to share data, preferably annonimised, for commercial purposes only after obtaining due consent from the user.**
   g. **For regulating and governing the Data Controllers they should be mandated to register themselves, through an online process, with TRAI.**
   h. **TRAI should impose suitable penalties, similar to TSPs, for any breach of privacy of the user.**
   i. **TRAI should be empowered to order blocking of content violating these norms.**
   j. **For effective regulation and governance, local hosting of apps and their data bases should be mandatory.**

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?

Our Response & Recommendations

Yes, it is most desirable to create technology enabled architecture to audit the use of personal data, and associated consent.

Yes, audit-based mechanism will provide sufficient visibility for the government or its authorized authority to prevent harm.

Yes, the industry can create a sufficiently capable workforce of auditors who can take on these responsibilities.

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?

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?

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?

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?

Our Response

Annonimization of data set is an effective measure that must be taken before encouraging the creation of new data based businesses consistent with the overall framework of data protection.

Yes, there is 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).

LEA requirements and usage of annonimized data can be considered as the legitimate exceptions to the data protection requirements imposed on TSPs and other providers in the digital ecosystem.

1. With the introduction of OTT services, the classical telecom services, viz, voice and messaging have been delinked from the underlying network. Even though the license for provisioning telecom services provides exclusive rights for voice and messaging services to the licensee, however, the revenue streams from these services have seen a constant decline forcing the TSPs to look for other avenues for generating revenues. Of late, analysis of the data generated by the individuals', be it their personal information or even their online activities have enabled targeted advertising to them, by the OTT services providers.
2. Though the licensees are the ones who create the individuals personal profile and also have the ability to monitor the individuals' online activity, yet they are prohibited for sharing of this information for commercial purposes. It is brought out that these days there are adequate techniques available that can annonimise the users' data yet be useful in providing adequate information that can be used for targeted advertising. **In order to establish parity between the licensed and unlicensed operators and to provide a reveneue earning opportunity for the licensed operators as well, the licensed operators too should be permitted to exploit their users data base for commercial purposes, albeit in an annonimized form.**

Our Recommendations

3. In view of the foregoing, it is recommended that,
   a. **Annonimization of data set is an effective measure that must be taken before encouraging the creation of new data based businesses consistent with the overall framework of data protection.**
   b. **Licensed operators too should be permitted to exploit their users data, in an annonimized form, for commercial purpose.**
   c. **LEA requirements and usage of annonimized data can be considered as the legitimate exceptions to the data protection requirements imposed on TSPs and other providers in the digital ecosystem.**

Question 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?

Our Response

No, government or its authorized authority should not setup a data sandbox, which allows the regulated companies to create anonymized data sets which can be used for the development of newer services.

1. Annonimization of datasets is a specialised stream of data analytics. There are plethora of niche companies existing today that provide highly advanced data annonimization techniques. These companies also have the capability to create dummy data which can be hired and used for development of newer services.
2. Additionally, it is brought out that licensed communication entities / data collectors are obligated to ensure security of the data of their subscribers. **It would be most prudent to allow the licensees / registered data collection entities itself to create**

the anonnimized data sets and lend the same for development of newer services instead of creation of any centralised sand box solution.

Our Recommendations

3. Therefore, it is recommended that,
   a. **Government or its authorized authority should not setup a data sandbox, which allows the regulated companies to create anonymized data sets which can be used for the development of newer services.**
   b. **The licensed operators should be permitted to create the annonimized data sets and provide them to entities wanting to develop newer services under commercial arrangements between them.**

Question 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?

Our Response & Recommendation

TRAI has recently launched a plethora of apps for speed testing, reporting of UCC, etc. A similar endeavour should be made by TRAI for setting up a technology solution that can assist it in monitoring the ecosystem for compliance.

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?

Our Response

1. Telecom eco-system encompasses the network elements, the software versions of these network elements, the BSS and OSS and even the user's handset and the apps installed in them. These create a lot of vulnerabilities for not only the user but the network as well. Having completed one license cycle, the vulnerabilities of the traditional telco network are well documented and adequate measures are available for mitigating them. Therefore, we would like to highlight the vulnerabilities that are arising due to the introduction of newer network technologies such as Network Function Virtualization (NFV) and the requirement of aligning the legacy encryption policies with the modern day encryption systems.
2. With the introduction of technologies like Network Function Virtualization (NFV), network functions which traditionally relied on hardware appliances are being transformed into software modules such as network firewalls and gateway routers / switches. Though "NFV[2] yields numerous benefits, particularly the possibility of cost-efficient transition of telco hardware functionalities on the software platform to break the vendor lock-in problem, however, these benefits come at the price of some security flaws. Indeed, **with NFV, virtual mobile networks become vulnerable to a number of security threats and are required to be addressed in the right earnest.**

[2] http://www.anastacia-h2020.eu/publications/NFV_Security_Threats_and_Best_Practices.pdf

3. From the point of view of encryption, it is brought out that the encryption policies enunciated by various sector regulators are at variance, as listed below, and there is a teething need to align the same to a single national policy.

   a. The Information Technology Act 2000 provides for prescribing modes or methods for encryption (Section 84A) and for decryption (Section 69).

   b. SEBI - Guidelines on Internet Trading

      i. Mandates the use of **64 bit / 128 bit encryption** for network security.

      ii. Recommends 128 bit encryption for both WAP based securities trading and internet based securities trading.

   c. RBI - Guidelines on Internet Banking. Mandates the use of SSL / 128 bit encryption as minimum level of security for Banks & banking transactions.

   d. DoT – Guidelines for Licensees

      i. Mandates evaluation and approval of encryption equipment.

      ii. Prohibits bulk encryption.

      iii. Level of Encryption limited by DOT to 40 bit key length.

      iv. For higher level encryption, DoT mandates seeking of written permission and deposition of Decryption Keys with them.

4. The dichotomy of these regulations is that on one hand the IT Act, 2000 stipulates adoption of internationally proven encryption techniques where as at the same time DoTs insistence on 40-bit encryption is outdated and poses major security risks. In this era of high speed computing devices, such instructions tend to be inconsistent with the International Standards and best practices. Therefore, **these is a need to ensure that,**

   a. **A single entity prescribes standardized encryption levels for attaining uniformity across services in India.**

   b. **Internationally proven encryption algorithms, such as a) DES 56 bits, (b) 3DES 128 bits and (c) AES 256 bits are adopted in India in consonance with the IT Act, 2000.**

   c. **Deposition of decryption key to be mandated with the CMS (Central Monitoring System) deployed by the Government to facilitate the real time monitoring by LEA's.**

Our Recommendations

5. In view of the forging, our recommendations are as follows,

a. **With introduction of newer technologies such as Network Function Virtualization (NFV), virtual mobile networks become vulnerable to a number of security threats and are required to be addressed in the right earnest.**

b. **For ensuring uniformity of encryption policy at the national level there is a need to,**

i. **A single entity prescribes standardized encryption levels for attaining uniformity across services in India.**

ii. **Internationally proven encryption algorithms, such as a) DES 56 bits, (b) 3DES 128 bits and (c) AES 256 bits are adopted in India in consonance with the IT Act, 2000.**

iii. **Deposition of decryption key to be mandated with the CMS (Central Monitoring System) deployed by the Government to facilitate the real time monitoring by LEA's.**

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?

Our Response

1. Digital services are a combination of the telecom services and IT services. The present day IT services are provisioned from a cloud setup that is location agnostic across the globe. Therefore, the security requirements for digital service shall necessarily have to be a combination of security measures enunciated for the telecom domain, IT domain as well as the cloud computing domain.
2. Telecom being a licensed activity in India, there are adequate time tested, auditable security measures in place that ensure due protection of users data and privacy. Foremost among them is the mandatory requirement of hosting of local data within the boundaries of India. **The measure has ensured adequate support for the LEAs and a similar approach is recommended to be adopted for addressing the jurisdictional challenges arising out of cross border flow of user's personal data and information.**
3. Since cloud based IT services are location agnostic across the globe, there is also a need to developed mechanisms for cooperating informally or, alternatively, resorting to what is typically referred to as requests for "Mutual Legal Assistance" for requesting and obtaining evidence for criminal investigations and prosecutions from a foreign sovereign state. Though India has MLAT agreements with 38 countries, as listed on the CBI site[3], provisioning of cloud based IT services shall mandate more of such MLATs.

[3] http://cbi.nic.in/interpol/mlats.php

4. MLATs apart, assistance may be denied by either country (according to agreement details) for political or security reasons, or if the criminal offence in question is not equally punishable in both countries. To obviate such situations, especially if the data hosting country is not inclined to India's interests, local hosting of servers and storage should be mandated for data collectors. India is the fourth largest country in terms of Internet users in spite of having an Internet penetration of a measly 6.9%[4]. Therefore, India is in the envious position to be able to leverage its market size for making other jurisdictions to legislate similar laws to ensure the security and privacy of data of its citizens and also force the data collectors to host their applications in local data centers.

Our Recommendations

5. In view of the above our recommendations are as follows,
   a. **For addressing the jurisdictional challenges arising out of cross border flow of user's personal data and information, local hosting of users personal data, especially by the data collectors, should be mandated.**
   b. **India should have maximum possible number of "Mutual Legal Assistance" agreements for getting information from data collector's setups hosted in cloud setups outside of India's territorial boundaries.**

[4] http://royal.pingdom.com/2010/07/27/top-20-countries-on-the-internet/