RSM/COAI/2017/206
November 06, 2017

Shri. Arvind Kumar
Advisor (BB&PA)
The Telecom Regulatory Authority of India
Mahanagar Door Sanchar Bhawan
Jawahar Lal Nehru Marg (Old Minto Road)
New Delhi-110002

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

Dear Sir,

1. This is with reference to the TRAI Consultation Paper dated August 09, 2017 on "Privacy, Security and Ownership of the Data in the Telecom Sector".

2. In this regard, please find enclosed our response for your kind perusal.

3. Please note that one of our member, Reliance Jio, has divergent views on some of the aspects mentioned in our response, on which the will be submitting their individual comments.

We hope that our views and submissions will merit the kind consideration and support of the Authority.

Regards,

Rajan S. Mathews
Director General

CC : Shri. Ram Sewak Sharma, Chairman, TRAI
: Shri. Sunil K. Gupta, Secretary, TRAI

14, Bhai Veer Singh Marg, New Delhi – 110 001
tel: +91-11-23349275 fax: +91-11-23349276 email: contact@coai.in website: www.coai.in

COAI

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

Released on August 09, 2017

Preamble

a. **National Security and Privacy:** National security and privacy issues are of paramount importance. Accordingly, the regulatory framework must ensure their primacy and it is strongly recommended that no exception should be made for any service provider, including the OTT communication service providers, while subjecting them to the rules to meet the national security and privacy norms, i.e. **same service same rule should be established for similar service providers.**

b. At present, there is a widely differing treatment accorded between telcos and other internet eco-system stakeholders as regards security compliance requirements. It should be noted that extensive and stringent security conditions are laid down and are required to be met by the licensed telcos. These include:

   i. Taking permission/approval of the licensor for any new service
   ii. Setting up Lawful Interception and Monitoring (LIM) systems
   iii. Restriction on switching of domestic calls/messaging from outside the country
   iv. Restriction on sending user information abroad
   v. Gives the Licensor the right to inspect the sites/network used for extending the service
   vi. Providing necessary facilities for continuous monitoring of the system, not employing any bulk encryption equipment; taking prior evaluation and approval of Licensor for any encryption equipment for specific requirements
   vii. Switching/Routing of voice/messages in P2P scenario
   viii. Responsibility for ensuring protection of privacy of communication and confidentiality of subscriber information
   ix. Quality of Service, Unsolicited Commercial communications, Complaint Redressal Mechanism, etc.

c. However, the other internet eco-system stakeholders who use data access channel of the telcos to reach to the customer with their services, including similar voice and messaging services are not subject to the security restrictions imposed on the telcos.

d. There is undoubtedly a need to ensure that these concerns are addressed and there is a level playing field amongst all the internet eco-system stakeholders. This may be done by ensuring that the regulatory framework applicable to OTT communications services is the same as that applicable to the communications services provided by TSPs.

e. The telecom service providers already have clauses in their licenses, which they have to abide for providing access to public networks, which are comprehensive and sufficient for connectivity.

f. It is suggested that such clauses, or as may be finally decided by the Government, should be applicable to all the players in the eco-system and applied in a uniform manner.

g. We note that the TRAI has already in its recommendations, on Cloud Computing recommended:

   i. The Government may consider to enact, an overarching and comprehensive data protection law covering all sectors.
   ii. This data protection framework, inter alia, may incorporate the following:
      - Adequate protection to sensitive personal information;
      - Adopt globally accepted data protection principles as reiterated by Planning Commission's Report of Group of Experts on Privacy 2012;
      - Provisions governing the cross-border transfer of data;

h. It is also pertinent to mention that MeitY has been dealing with the issue of data security and privacy and the telecom service providers apart from their license conditions have to also comply with the provisions of the IT Act. Also, MeitY has recently constituted a committee of experts to deliberate on a Data Protection Framework for India.

Issues for Consultation

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?**

COAI Response

a. The data protection, privacy and confidentiality provisions under Unifed License are as below:

37. Confidentiality of information:

37.2 Subject to terms and conditions of the license, the Licensee shall take all necessary steps to safeguard the privacy and confidentiality of any information about a third party and its business to whom it provides the Service and from whom it has acquired such information by virtue of the Service provided and shall use its best endeavors to secure that:
a) No person acting on behalf of the Licensee or the Licensee divulges or uses any such information except as may be necessary in the course of providing such Service to the Third Party; and
b) No such person seeks such information other than is necessary for the purpose of providing Service to the Third Party.

Provided the above para shall not apply where:

a) The information relates to a specific party and that party has consented in writing to such information being divulged or used, and such information is divulged or used in accordance with the terms of that consent; or

b) The information is already open to the public and otherwise known.

37.5 The use of encryption by the subscriber shall be governed by the Government Policy/rules made under the Information Technology Act, 2000.

39.23
(viii) The Licensee shall not transfer the following to any person/place outside India:-

a. Any accounting information relating to subscriber (except for international roaming/billing) (Note: it does not restrict a statutorily required disclosure of financial nature); and
b. User information (except pertaining to foreign subscribers using Indian Operator's network while roaming and IPLC subscribers).

b. Thus, insofar as the interests of the telecom subscribers are concerned, these are prescribed and protected only qua their respective service providers. Unified License of the Telecom Service providers contains several conditions pertaining to security, data protection, privacy, confidentiality, etc. which a Licensee has to abide by in providing connectivity to its subscribers, which are comprehensive and sufficient for data protection.

c. **Therefore, there is no need for any additional requirements on the TSPs as existing conditions in Unified License are sufficient, as submitted above.**

d. However, as submitted above, the data protection requirements are not uniformly applicable to all the players in the eco-system in India.

e. The regulatory framework must recommend that no exception should be made for any provider of communication service while subjecting them to the rules to meet the data protection and privacy norms, i.e. **same service same rules should be established for similar service providers.**

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?**

COAI Response

a. **The IT Act defines information, personal information and Sensitive personal information separately as given below:**

i. "Information" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche; (Amended vide ITAA-2008)

ii. "Personal information" means 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.

iii. "Sensitive personal data or information" (SPI) means such personal information which consists of information relating to, inter alia 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.

b. We believe that the above definition under the IT act is sufficient and may be continued with.

c. We believe that any privacy and data protection law should acknowledge a distinction between the `Personal Information or Personally Identifiable Information (PII)' and `anonymized or aggregate data. The User's consent should be required only if his/her data is being shared in any user identifiable format. In case of anonymized data, we believe that no consent is required, except that the Privacy policy of the organization will mention the recipient and purpose of sharing/use of such data.

d. The customers right to be forgotten should be addressed by facilitating deletion of personal data (expect that is required to be stored as per law) once the customer wish to terminate the services.

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.

COAI Response

a. In case of TSPs, they are the data controllers and they inform the users while collecting information that the information is being collected and the purpose for which the information is being collected.

b. However, in case of other digital entities, a set of regulatory principles need to be set for them to act as data controllers.

c. The same priciples, as finally decided, should be applicable to Telcos as well as other digital entities.

d. As submitted above, specific consent may not be required for use of information in an anonymized format.

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?**

&

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?**

COAI Response

a. It is important that fears relating to abuse of data of the public should be countered by encouraging good practices and transparency.

b. However, we believe that it would be difficult to create a technology enabled architecture to audit the use of personal data, and associated consent must be created.

c. We suggest that instead, adherence to rules may be audited by the companies internally or by third parties such as accredited standards bodies like ISO for security; or by auditing firms that have the requisite expertise and capability.

d. The format, structure, periodicity of such certification, may be decided in consultation with the stakeholders.

e. Needless to say such audits for data protection and consent certification should be required for all players in the eco-system.

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?**

COAI Response

a. Big data and analytics is an emerging area that can deliver immense societal and economic benefits for Social Good and Nation Building and also to improve operational efficiencies and effectiveness in various areas such as:

i. Solving traffic problems in cities, resolving traffic congestion, smart parking
ii. Targeting healthcare delivery, controlling disease spread
iii. Disaster management, emergency evacuation on natural calamities
iv. Efficient supply chain management,
v. Preventive steps for environmental protection,
vi. Providing a personalised educational experience for students,
vii. Enabling security to individuals and society at large, and
viii. Informed policymaking

b. This will also go a long way in facilitating country's objectives of Smart Cities, Digital India whereby big data analytics can help Government/ Economy in better social good and mechanism for disaster management in emergency situations.

c. A clear regulatory framework, clearly, consistently and uniformly applied to all players in the eco-system is a must for level playing field.

d. The framework should be light touch and future fit so as to facilitate rather than inhibit innovation.

e. An ex post rather than ex ante approach is desirable.

f. A stringent approach should be confined to a small negative list in respect of matters pertaining to national security.

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?

COAI Response

a. No, we believe that the Government or its authorized authority should not setup any data sandbox for companies to create anonymized data sets which can be used for the development of newer services. Each entity should be responsible for the data that they own. Governmental or regulatory bodies should rather act as catalysts and facilitators to help market and negotiation-based solutions to take off.

b. It may however be useful if Government data is made available in a Government sandbox in anonymized data sets as this can then be leveraged by companies to create innovative use cases.

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?

COAI Response

a. Extensive and stringent security conditions are laid down and are required to be met by the licensed telcos However, the other internet eco-system stakeholders who use data access channel of the telcos to reach to the customer with their services, including similar voice and messaging services are not subject to the same security restrictions as are imposed on the telcos.

b. There is undoubtedly a need to ensure that these concerns are addressed and there is a level playing field amongst all the internet eco-system stakeholders. This may be done by ensuring that the regulatory framework applicable to OTT communications services is the same as that applicable to the communications services provided by TSPs.

c. Collective industry action is required to protect connected networks and consumers through consistency and consensus in the development of standards and the proportionate use of monitoring, detection and blocking capabilities

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?**

COAI Response

a. While telcos are subject to stringent data protection requirements along with strong licensing and regulatory oversight, the same rules are not applicable to the OTT players or other players in the ecosystem such as device manufacturers, operating systems, browsers etc.

b. A ubiquitous data protection regulation, applied uniformly to all, will go a long way towards addressing concerns regarding differential treatment, differential rules, etc.

c. There is a need to harmonize the data protection requirements under various laws/rules and bring then under a common data protection framework.

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?**

COAI Response

a. Yes, there a need for bringing about greater parity in the data protection norms applicable to TSPs and other communication service providers offering comparable services.

b. National security and privacy issues are of paramount importance. Accordingly, the regulatory framework must ensure their primacy and it is strongly recommended that no exception should be made for any service provider/player in the ecosystem, including the OTT communication service providers, while subjecting them to the rules to meet the national security and privacy norms, i.e. **same service same rule should be established for similar service providers.**

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?**

COAI Response

a. Publicly available data and anonymized data should continue to be excluded from the purview of data protection requirements.

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?

<u>COAI Response</u>

a. The license of the TSPs restricts the telecom operators to send any user identifiable information (including the data can have an impact on national security)outside India. The telecom operators are only allowed to use cloud services as an Enterprise. However, similar or more information pertaining to identification of the subscribers is being sent outside India through subscribers themselves or through handsets or websites.

b. The volume and characteristics of cross-border data flows are evolving, elevating privacy risks and the need for improved law enforcement co-operation. While this is exposing individuals to more privacy risks, it is also challenging businesses which are collecting the data directly entered by users, or through their actions without their knowledge, - e.g. web surfing, e-banking or e-commerce – and correlating the same through more advanced analytic tools to generate economic value out of data. Thus, there is a need to maintain level playing field and the principle of same service same rules.

c. The Government may consider limiting certain data (such as biometric data, data related to critical infrastructure) to remain within the country in order to protect national security requirements and to safeguard the public interest.

d. **Further, to address the issue of access to data, hosted by CSPs in different jurisdictions, by law enforcement agencies, we note that the TRAI in its recommendations on cloud Computing, has already recommended that:**

   i. **Robust MLATs should be drawn up with jurisdictions where CSPs usually host their services, enabling access to data by law enforcement agencies.**
   ii. **Existing MLATs should be amended to include provisions for lawful interception or access to data on the cloud.**
   iii. A similar approach may be recommended in respect of **jurisdictional challenges pertaining to cross border flow of information in the digital ecosystem.**

****