RELIANCE JIO INFOCOMM LIMITED'S (RJIL) COMMENTS ON TRAI'S CONSULTATION PAPER ON "PRIVACY, SECURITY AND OWNERSHIP OF THE DATA IN THE TELECOM SECTOR"

(Consultation Paper No 09/2017 Dated 9th August 2017)

General Comments:

1. RJIL welcomes the Authority's decision to issue this consultation paper to deliberate the efficacy of current measures for data privacy and data security and to identify key issues pertaining to data protection in relation to the delivery of digital services. The issue of data privacy and data ownership is very topical, as it is not only grabbing newspaper headlines but is also a matter of multiple litigations. The quantum of sensitive data being generated every day makes it imperative to have clear guidelines on the use and storage of such data. Therefore evolving a guiding policy framework is imperative.

2. At the outset, we bring to the Authority's kind attention that the concepts of data privacy, data security and data ownership have wide ranging and multi sector implications and any discussion about these issues should be done at a holistic level, involving various sectoral stakeholders.

3. The Authority has rightly taken note of the various Data privacy and Data security regulations already in place. Starting with the Indian Telegraph Act, 1885, the terms and conditions of the Unified License, TRAI Direction of 2010 and the Information Technology Act, 2000 collectively define the comprehensive regulatory oversight for data privacy and security, applicable for TSPs.

4. In addition to this, the license provisions regarding collection and maintenance of commercial records/ Call Detail Record (CDR)/ Exchange Detail Record (EDR)/ IP Detail Record (IPDR) and the requirements for traceability of subscribers and the instructions and procedures for sharing customer details with the Law Enforcement Agencies (LEAs) provide a definitive framework on sharing the subscriber's personal data. Thus clearly, the licensees are already operating under a well-defined and well-thought regulatory regime with regards to data privacy and security.

5. However, from the perspective of laying the foundation of an all-encompassing policy framework, we agree with the Authority that the recommendations by the Group of Experts headed by (Retd.) Justice A. P. Shah, vide report dated October 2012, to the Planning Commission on the subject of data privacy could be a good starting point. We also believe that these recommendations would be useful in examining the soundness of the current framework governing the protection of user data across various other stakeholders in the digital ecosystem.

6. We also believe that the comprehensive policy framework for data protection should be developed keeping in mind the challenges posed by new concepts like "big data" and unlicensed activities carried out by Over the top ("OTT") service providers and Cloud service providers. We should also be conscious of data traceability, especially given cross-border transfer of a lot of sensitive data and lack of jurisdiction in such instances.

7. The need for a principles based approach is necessitated by the existence of various unlicensed and unregulated entities that handle or process personal and sensitive data of telecom customers. These can be the OTT service providers, which ride over the telecom networks and collect a large amount of personal information through their applications. These can be the device manufacturers that collect the fingerprints, voice samples, facial features etc. to provide assistance to the subscribers and help secure the subscriber devices. The device manufacturers also collect a large amount of data for analytics etc. Similarly, the cloud service providers collect and store enormous amount of consumer data. However, as most of these entities are unlicensed entities, these are not being regulated today, and current regulations have little impact on their activities. This is an important matter that the Authority should look into to ensure protection of data as well as for the critical objective of national security.

8. Internationally, the broad jurisprudence around data privacy and data security laws is based on a few fundamental common features. The primary among these is that personal data can be gathered by any agency for a legitimate purpose only. Post collecting the personal data, the agencies responsible for collecting and storing the personal data are deemed responsible for protecting the same from misuse and pilferage. In addition to this there are certain rights assigned to the data owners.

9. The international directives and regulations on data privacy and related issues are generally not industry or sector specific, instead these are implemented on a country wide level. The European Union ("EU") members are currently following the 2012 Directive (also known as Cookie law) with country specific modifications. These will be replaced by General Data Protection Regulation ("GDPR"), effective May 2018. Overall around 80 countries, including many countries in Latin America and Asia, have adopted comprehensive data protection laws.

10. The European regulation states that besides personal data collector, any entity that processes the personal data will also be responsible for its protection, including third parties such as cloud providers. Thus any entity that ever comes in any sort of contact with the personal data becomes responsible in case of data breach. The ramifications of this measure is that the unlicensed service providers are also responsible for data security. This regulation also affects global organizations operating in EU, which may have data on EU citizens and residents. This regulation delves into the aspect of cross-border transfer of data as well, which is critical, as any amount of regulation and policy will be rendered useless if the data is easily transferred cross-border, where the domestic authorities have no jurisdiction. The proposed British statement of intent on new Data Protection Bill goes one step ahead of the GDPR, as it proposes to treat the intentionally or recklessly re-identifying individuals from pseudonymised and anonymised data and altering records in the wake of a Subject Access Request (SAR) made by the Data Subject as a criminal offence.

11. Cross border transfer of data is a critical issue prompting many international legislations to protect sovereign interests. Russia and China have already implemented laws on local hosting of the data and the same is on the anvil in Europe. In fact China has proposed an additional draft law requiring any foreign owned entity to certify that any data taken out of China's borders will

not impact national security or interests. We submit that it is imperative that cross border transfer of sensitive data be prohibited by promoting localized hosting of personal data in India as is being done in the case of Aadhaar data. We reiterate the risk of all the regulations being rendered futile if operators are able to transfer data outside the country as then the local authorities / regulators will have little jurisdiction. There are several operators today who do not even have a presence in India and yet are able to transfer data outside the country. The only way to protect the interests of consumers and national security will be through firm laws on local hosting of data as has been done in several countries already.

12. Conclusion:

1. **The regulatory framework to ensure data privacy, data security and data ownership is well defined for the TSPs.**

2. **The Authority may evolve an all arching comprehensive principles based guidelines applicable for all sectors in consultation with other relevant sectoral regulators. There should be no compromise with the requirements to ensure national security.**

3. **There is an imminent need to bring the OTT players and other unlicensed service providers collecting consumer data under the Data Privacy principles umbrella.**

4. **The Authority should put in place measures to curb cross-border transfer of data by mandating localized hosting of data.**

Issue wise response:

Q. 1 Are the data protection requirements currently applicable to all the players in the eco-system in India sufficient to protect the interests of telecom subscribers? What are the additional measures, if any, that need to be considered in this regard?

RJIL Response:

1. We submit that with increase in digitalization, numerous organizations collect, store and process data in various forms and shapes. With large number of players in the digital ecosystem, it is extremely important to ensure personal data protection, in order to ensure privacy to a user. This becomes more significant in view of privacy been recognized as a fundamental right by the Hon'ble Supreme Court. However, as of date, in India we do not have a comprehensive Data protection/ personal data law.

2. As detailed in the general comments, TSPs are already mandated to ensure security of customer data and privacy by various provisions of the Indian Telegraph Act, the Information Technology Act and License terms and conditions and the TRAI directions.

3. The Indian Telegraph Act 1885 prevents unauthorized interception of messages and requires the Licensees to maintain secrecy. It, inter alia, requires the service providers to put in place adequate and effective checks to ensure that unauthorized interception of message does not take place, unless by law enforcement agencies.

4. The Unified License, under clause 39.4, Chapter VI, mandates the licensees to ensure the protection of privacy of communication and ensure that unauthorized interception of messages does not take place. It also mandates the Licensees to ensure the confidentiality of Information. The licensee is also required to maintain all commercial records/ Call Detail Record (CDR)/ Exchange Detail Record (EDR)/ IP Detail Record (IPDR) with regard to the communications exchanged on the network for at least one year.

5. TRAI direction of 2010 also mandates the TSPs to ensure confidentiality of information as provided in the license conditions and to put in place appropriate mechanisms so as to prevent breach of confidentiality of information of the subscribers and privacy of communication.

6. **Thus, we submit that there is adequate regulatory oversight to ensure data privacy and data security of customer data as well as customer communication for the licensed service providers.** However, the same cannot be said of other players in the ecosystem to which these laws do not apply. The provisions governing data privacy and security are not sufficient for such entities collecting personal data of the subscribers and the only relevant provisions governing these entities are the IT act and IT rules.

7. The international practice is to cover all sectors and personal information collectors and processors under single overarching principles based regulatory framework to ensure equity in law. Globally, a lot of countries have legislated Privacy and Data Protection Acts, which are not sector specific but are based on “horizontal principles”. Some of such data protection laws are highlighted below:

    i. The **EU** has adopted the “EU General Data Protection Regulation” which is due to come into force on 25th May,2018;

    ii. **Singapore** has the “Personal Data Protection Act 2012”;

    iii. **Australia**, through Privacy Act of 1988, has 13 legally binding principles known as Australian Privacy Principles (APPs). The APPs set out standards, rights and obligations for the handling, holding, use, accessing and correction of personal information (including sensitive information);

iv. **Japan** has the Act on Protection of Personal Information (APPI) 2003 which has applied to the private sector since 2005. The law covers both the public and private sectors;

v. **South Korea's** privacy law is contained in the Personal Information Protection Act (PIPA) 2011, a comprehensive data protection law. PIPA was amended in 2013, 2014 and 2015;

vi. The Federal Trade Commission Act (FTC Act) of the **United States of America** is a federal consumer protection law that prohibits unfair or deceptive practices and has been applied to offline and online privacy and data security policies.

8. **The above examples highlight that the data protection guidelines should be principle based and should not be sector specific.** These should be overarching so that every organization ensures that the customer privacy is maintained by adopting these principles in line with their operational activities.

9. While a comprehensive national framework may develop, the Authority should develop regulations for any service provider which is in the telecommunication and digital services related eco-system. The Authority can regulate entities, such as OTT applications, that are providing services riding on the telecommunications networks and to the same set of subscribers that are being served by the licensed entities. The Authority should consider means to ensure compliance by these other service providers of the data privacy and security laws. There are certain critical aspects, such as data misuse, cross-border transfer of data, commercial utilization of data etc that the Authority should prevent urgently.

Q. 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?

RJIL Response:

1. The Government of India had notified **"Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011"**. As defined in these rules, "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. According to **Rule 3** of this notification, "*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*"

2. RJIL submits that the above mentioned rules (as part of IT Act) satisfy the contours of personal data definition. We also suggest, that any further addition or changes to the definition should be technology/ service neutral and the definition should be applicable to all the players in the digital ecosystem, irrespective of the organizations origin (based in India or not) or them being under the Government's licensing regime (or not).

3. We further submit that any kind of processing of personal data should be fair and transparent. Providers of personal information should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. Particularly, the specific purposes for which personal data is processed should be explicit and legitimate as well as determined at the time of collection of personal data. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, which includes preventing unauthorized access to or use of personal data and the equipment used for the processing.

4. The user's personal data should not be used for commercial purposes, without explicit consent. The consent thus taken should be purpose-limited as per recommendations of AP Shah Committee. The Aadhaar based eKYC being done by RJIL and other telecom service providers can be used as holistic case based practice that could be followed elsewhere.

5. As an exception to the policy, anonymized data should not be considered as "*personal data*", since the same has been rendered identity-less. The guidelines for data protection should provide for sharing or processing of such kind of anonymized data as it will not only help the policy initiatives but can be used by different businesses in giving a better experience to the end user(s) in whatever services are being offered by them.

6. As a TSP, the provider of personal data is given rights to edit/ correct his/her data provided to the service providers. The regulatory and judicial framework also provides for accommodating any changes to the personal data. The Unified License conditions prevent misuse of the personal data collected by a licensee. Thus, in our opinion, users registered with TSPs have relevant and sufficient control over their personal data.

Q. 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.

RJIL Response:

1. We submit that, as far as the licensed telecom services are considered the distinction between the rights and responsibilities of the data controller vis-à-vis the rights of the telecom subscriber can be easily derived from the provisions of the Unified License.

2. With regards the framing of guiding principles for data privacy, the first and foremost requirement is to define the Data Controllers, as different agencies through their operational functions collect, store and process data in difference forms and formats.

3. The **EU General Data Protection Regulation** (approved by the EU Parliament on 14 April 2016, enforcement on 25 May 2018) can be used as a reference; as per **Article #4 of EU GDPR**:

   i. *'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;*

   ii. *'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;*

   iii. *'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;*

   iv. *'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;*

   To do justice to the ecosystem, the above defined four terms – 'controller', 'processor', 'recipient' and 'third party' may be used interchangeably for the same organization as it may have the capabilities qualifying it for all the four definitions.

4. It becomes extremely important that the Rights & Responsibilities be defined for the above mentioned entities to safeguard data and ensure compliance by the entities, in addition to their usual activities.

5. **Article #21 of the EU GDPR** might serve as a reference, wherein the controllers, processors or third parties are responsible to implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the regulation. It also lays down a code of conduct in reference to these entities.

6. The EU GDPR also calls for implementation of appropriate data protection policies and puts the responsibility on the entities to demonstrate compliance whenever asked for by the regulator.

7. Basis reference from the EU GDPR and AP Shah committee report, the principle based guidelines for data protection should also provide for:

    i. Supervisory authorities – which can conduct audits and supervise for driving compliance; for telecom sector, the Authority and the DoT are the natural supervisory authorities.

    ii. Certification bodies – which may set up standards and certification programs for the entities and help them become self-sufficient as far as compliance is considered

8. The Rights of Data Subject (to whom the personal data pertains) should always supersede the Right of Data Controllers, barring scenarios pertaining to national security. The Data Controller/ Processor should not disclose/ process/ transfer personal data of the Data Subject to any other entity/ organization/ third party without the explicit consent of the Data Owner, barring the designated LEAs. The following could be excused from the consent requirements:

    i. Anonymized data should be given an exception to the above practice;

    ii. In cases of National Security or Safeguarding of Public Interest as required by Law Enforcement Agencies, as already included in the Licensing Terms & Conditions

9. Another important aspect is that an individual / customer should be able to access his/ her data at any point of time or require the Data Controller to return and destroy such data. This should be an obligation of the Data Controller and the Authority should be able to satisfy itself that this condition has been met. The Authority (or the relevant Indian Government agency) should be able to enforce such a requirement, with ability to track the data flow.

Q. 4 Given the fears related to abuse of this data, is it advisable to create a technology enabled architecture to audit the use of personal data, and associated consent? 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?

&

Q. 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?

RJIL Response:

1. Given the pace of technological advancement, an architecture or setup designed today might need fundamental changes within a short period of time. For example, with the advent of AI and Blockchain based technological initiatives, a lot of organizations are changing the way they used to collect, process and store data. Thus, it would be logical and in the interest of the public at large, that the guidelines for data protection should not define the setup but give a principle led approach to the industry for the design and implementation of such a setup. In fact, the focus should be to encourage concepts like 'Security by Design'.

2. The Authority, though, could supervise and oversee that such mechanism, whenever developed and deployed, follow the principles of data protection and usage as suggested by the AP Shah Committee.

3. The Authority could also proceed with empanelment of:

   i. "Certification agencies" that follow global best practices and can enable the industry players with standardized certificates. For example, the ISO 27001 for Information Security can be one such case based certificate;

   ii. "Auditors" that can help industry with the compliance effectiveness for the same.

4. The industry is always working on implementing latest technologies which result in consumer satisfaction and build business proficiencies. These also lead to creation of skill pool around the technologies. Thus industry would be able to provide skilled manpower to develop, deploy, supervise, certify and audit these practices. This will also result in skill development and employment generation within the country.

5. All TSPs should be committed to safeguarding the consumer personal data and should be encouraged to follow global best practices in implementing a state of the art architecture with regular auditing of facilities with the help of internal as well as external auditors, thereby reassuring the consumers regarding safekeeping of their personal data.

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

&

Q. 6 Should government or its authorized authority setup a data sandbox, which allows the regulated companies to create anonymized data sets which can be used for the development of newer services?

RJIL Response:

1. We submit that with the pace of technological advancements, the speed & skills required to implement a sandbox would be best provided by different players in the industry. The Government should refrain from micro management.

2. With rapid pace of technological changes, many organizations are coming up with innovative business models based on customer behavior and in order to enhance customer experience. While every organization is seeking to become digital, customer data collection, processing and storage is also becoming an operational need with all businesses. "*Big data*" and analytical modelling are getting bigger by the day with interlinked data privacy issues and challenges. Thus it is safe to accept that the consumer demands will help create best suitable sandbox algorithms to help address these issues.

3. Further, as is evident from the Authority's experience, light touch regulatory approach in the Telecom & IT sector has allowed for both – innovation for the businesses and ease of usage for the customers. Thus, it would be prudent and in public interest to continue following these successful mantras and help the private sector build models around anonymized data.

4. As submitted before, the Authority should share a principle based guideline for the industry to develop such mechanisms which could be followed up with auditory supervision and compliance testing.

Q. 8 What are the measures that should be considered in order to strengthen and preserve the safety and security of telecommunications infrastructure and the digital ecosystem as a whole?

RJIL Response:

1. We submit that while digital convergence has benefitted consumers, it has also created regulatory challenges by introducing various third party and unregulated players in the market with cross border operations and affiliations. The complexity of fast changing digital ecosystem has given rise to regulatory uncertainty, and the rapid pace of change leads to regulations becoming obsolete in a short span of time.

2. In the interest of National Security and Customer Data Privacy, the guidelines for data protection should also provide for data localization for sensitive data i.e. the collected data should be processed and stored in servers located in India only. This would give a sense of protection and assurance to the consumers that their personal data is safe and secure; and

that the consumers would have access to judicial remedies in case the same is misused. This practice would also strengthen the regulators by helping them to keep a close watch on the activities of the different players involved in the ecosystem.

3. With the increase in cyber related criminal activities, it has become very important that cyber security be taken as a component of the regulatory framework. The guidelines must therefore enforce security related checks and balances with all the players of the ecosystem, with effective safeguards build into it to prevent misuse.

4. Policymakers all over the world are now recognizing the associated challenges and working to implement reforms that will protect competition and consumers without impeding social and economic progress. Some of the principles which are being globally adopted are as follows:

   i. **Privacy by Design:** This approach ensures that 'privacy' is a central part of the entire framework and gets embedded into the system right from the inception. GSMA has published a comprehensive document titled "Privacy Design Guidelines for Mobile Application Development" that articulates the Mobile Privacy Principles in more functional terms and is intended to help drive a more consistent approach to user privacy across mobile platforms, applications and devices.

   ii. **Technology Neutral / Platform Neutral Regulation:** This approach requires that the regulations should be designed to achieve its objective in the most efficient way without regard to technologies, industry structures, or legacy regulatory regimes. This helps avoid uncertainties in light of rapid technological changes and evolving businesses.

   iii. **Innovation led Light Touch Approach:** The fact is that digital ecosystem is dynamic and complex and is continually evolving. This is leading to rapid innovation in each and every stream of the ecosystem. Many a times, the developments are such that regulatory bodies need to allow enough breathing space so as to allow the evolution of the ecosystem. In the long term, regulations could be tweaked for better results but overbearing approach might lead to a road block in development of both the technology as well as businesses at large.

Q. 9 What are the key issues of data protection pertaining to the collection and use of data by various other stakeholders in the digital ecosystem, including content and application service providers, device manufacturers, operating systems, browsers, etc? What mechanisms need to be put in place in order to address these issues?

RJIL Response:

1. With each passing day, organizations are increasingly trying to collect as much personal data to give the users a "personalized experience." Also, as the Internet of Things continues to grow,

organizations are faced with more and more ways to collect more and more kinds of data, including and especially private, personally identifiable data.

2. Data collected by almost all the eco-system players can be classified as personal data or more so as sensitive personal data. Thus, it is in public interest that the guidelines for data protection should address all the players in the digital eco-system which are becoming custodians of "enormous" personal data being collected at each and every instance. As Telecom Service Providers, we are already following our obligations as per the existing laws and regulations and are being audited for the same by the regulator and other government agencies.

3. In the interest of national security and consumer privacy, Data Localization should be one of the most important aspects of the framework. Different players in the ecosystem collect, process and store data in servers outside the geographical boundaries of India. This results in undue judicial delays even in case of regular enquiries leading to a situation which results in dilution of powers of the law enforcement agencies. Also, with the increase in applications providing encrypted message delivery, the law enforcement agencies are at a loss. Thus, the guidelines should consider the framework wherein data is collected, stored and processed in India so that the security of the ecosystem can be strengthened. This would also lead to a sense of assurance for the consumers as it would give them access to judicial remedies in case the situation demands, unlike in the current scenario.

4. Another key feature could be accountability for the data being collected, processed and stored. This should be ensured in letter and spirit by the new guidelines. The data collector/ processor should be held accountable for any breaches or unauthorized access to personal data.

5. "Data minimization" could be another guiding principle for organizations involved in data collection. Data minimization refers to the practice of limiting the collection of personal information to that which is directly relevant and necessary to accomplish a specified purpose. This could be understood using Principle 3 propounded by Information Commissioner' office ("ICO") which is UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The principle states, "*Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed*". Similar principle is also mentioned in EU GDPR. The use of data minimization ensures that the data collector sticks to collecting the data which is of utmost importance to the performance of the app/ website etc. but not beyond that.

6. The guidelines could also aim to introduce the data owner's right to object, wherein personal data is processed for direct marketing. This would ensure that the data owner is made sufficiently aware of the commercial interest that comes along with processing of their personal data and would also ensure that the data collected for a purpose is not misused by the collector for any purpose other than that consented for.

Q. 10 Is there a need for bringing about greater parity in the data protection norms applicable to TSPs and other communication service providers offering comparable services (such as Internet based voice and messaging services). What are the various options that may be considered in this regard?

RJIL Response:

1. We submit that there are two types of communication service providers. First group is the licensed TSPs and the second group consists of unlicensed OTT players. While the TSPs are required to obtain a license and abide by all the license conditions, the OTT players can start their operations even remotely with no oversight of the regulatory agencies. The TSPs are required to comply with comprehensive license terms and conditions and with the Authority's regulations/ orders/ directions including those on data privacy and security.

2. Most of the OTT service providers, be it browser based or application based, providing communication services within India, have their servers outside the country, which leaves Indian security agencies powerless to exercise their rights in case of security compliances. Such practice of having servers outside the country also endangers privacy of the Indian Citizens' personal and/or sensitive data since service provider operating in a particular country is bound by its legal system. The laws of that country may force such service provider to permit the legal officials of that country to access the data and any encryption keys that are stored within the nation's geographical boundaries. Even if the service providers and/or security agencies try to capture the information flowing in the network, they can get only the raw data, as most of the OTT players use special encryption and it is extremely difficult for the Government and service provides to obtain decryption keys. Previously, the Authority has cited the protracted negotiation between security agencies and a specific device company. Therefore, some sort of regulatory framework needs to be evolved so that National Security and consumers' security, safety and privacy issues are addressed along with ensuring the independence and ease of being a developer of the OTT applications and services.

3. We submit that the Authority may consider evolving a suitable regulatory oversight for the OTT communication service providers for the rules pertaining to data privacy and data security. The prevailing situation results not only in uneven business conditions, but also allows unscrupulous elements in their anti-national and un-lawful activities by aiding them directly or indirectly through their communication services. Thus, the guidelines for data protection should address this anomaly and should put in place rules on data privacy and data security for all types of service providers be it licensed or unlicensed entity.

Q. 11 What should be the legitimate exceptions to the data protection requirements imposed on TSPs and other providers in the digital ecosystem and how should these be designed? In particular, what are the checks and balances that need to be considered in the context of lawful surveillance and law enforcement requirements?

RJIL Response:

1. We reiterate our submissions in response to previous questions that data sharing with the designated LEAs, in compliance with applicable provisions, and data collected for the purpose of national security may be exempted from data protection requirements. Additionally as the anonymized data is identity less, it should be granted an exception from data protection requirements.

2. We also submit that at present the OTT communication service providers are fully exempted from any such data protection requirements and therefore a grave security threat. We reiterate that these service providers should be brought under the regulatory oversight to help bring in policy uniformity in implementation of lawful surveillance and law enforcement requirements.

Q. 12 What are the measures that can be considered in order to address the potential issues arising from cross border flow of information and jurisdictional challenges in the digital ecosystem?

RJIL Response:

1. The aspect of cross border flow of data may be viewed with a perspective of rapid globalization and the need of scale in communications networks in order to deliver far greater business efficiencies and convenience for users. However, in no case this should be allowed at the cost of National Security. Therefore it is imperative to mitigate such risks while at the same time ensuring the trust needed in a global economy dependent on the free flow of information by implementing strong cross-border privacy law enforcement.

2. Globally, different nations are sensing the need of greater protection of personal data and are coming up with initiatives to have localized data storage and processing capabilities. These also result from the fact that cross border jurisdiction does not apply and is not respected in different geographies. This results in long term judicial litigations and have the ability to cause long term harms to individuals as well as the countries.

3. As stated in our earlier responses, National security and Privacy of Customer are matters of utmost importance and hence, cross border transfer of sensitive personal information/ data should be prohibited.

4. **China's** new Counter-Terrorism Law requires Internet and telecommunication companies and other providers of "critical information infrastructure" to store data on Chinese servers and to

provide encryption keys to government authorities. Any movement of data offshore must undergo a "security assessment."

5. **Indonesia** has introduced general data localization requirements related to data processed for public services. Article 1 of the Draft Ministerial Regulation concerning Data Center Technical Guidelines states that "*Any Electronic System Administrator for public service shall place a data center and a disaster recovery center in Indonesia*." Also, Article 17 (2) of the Regulation on Electronic System and Transaction Operation states that "*Electronic System Operation for public services shall place a Data Center and disaster recovery center in the territory of Indonesia for law enforcement, protection and sovereignty of the state and its citizens*."

6. From September 2015, it is a legal requirement that data operators store the personal data of Russian citizens on servers based in **Russia**. The *Roskomnadzor* is tasked with implementing this law. Large foreign-based data operators have been given time to comply with the law.

7. Cross-border transfers are forbidden unless they satisfy certain requirements - most notably that the recipient is subject to a law, code or contract that ensures a level of privacy protection equivalent to that of **South Africa**.

8. The **Canadian** provinces of British Columbia and Nova Scotia have implemented laws mandating that personal data held by public bodies such as schools, hospitals, and public agencies must be stored and accessed only in Canada, with some minor exceptions.

9. Data controllers must register with the **UK's** Information Commissioner's Office to report their intention to process personal data before they begin. Fees and an annual renewal requirement apply. The Data Protection Act allows limited data to be transferred to non-EU countries, that too subject to a range of conditions.

10. The above mentioned global laws do highlight the fact that data localization is being increasingly adopted by different nations. We should also have a similar policy wherein sensitive data of Indian citizens should be processed and stored in servers within our geographical boundaries.