**Bharti Airtel Ltd.**
India & South Asia
Airtel Center, Plot No. 16,
Udyog Vihar, Phase - IV,
Gurugram - 122 015

www.airtel.in
Call +91 124 4222222
Fax +91 124 4248063

Ref No: RP/FY 17-18/062/406
Dated: 06th November, 2017.

**To,**
**Shri Arvind Kumar,**
**Advisor (Broadband & Policy Analysis),**
Telecom Regulatory Authority of India,
Mahanagar Doorsanchar Bhawan,
Jawahar Lal Nehru Marg,
New Delhi – 110 002.

**Subject: Response to Consultation Paper on "Privacy, Security and Ownership of the Data in the Telecom Sector".**

**Reference: TRAI Consultation paper dated 09th August, 2017.**

Dear Sir,

This is with reference to your above mentioned consultation paper. In this regard, please find enclosed our response for your kind consideration

Thanking you,

Yours Sincerely,
For **Bharti Airtel Limited.**

**Ravi P. Gandhi**
**Chief Regulatory Officer**

**Enclosed: As mentioned above**

## Bharti Airtel Limited's Response to TRAI's Consultation Paper on 'Privacy, Security and Ownership of the Data in the Telecom Sector'

At the outset, we thank the Hon'ble Authority for providing us with an opportunity to submit our views on this Consultation Paper.

The Internet and the digitalization of services/processes are driving the digital transformation of India by empowering the society and contributing to the Nation's Economic Development. The Digital Economy or the Internet Economy is increasingly influencing our social and economic activities and even the way individuals live and connect. This digital transformation offers ample opportunities for implementing radical new approaches in healthcare, transport, education, agriculture, energy, e-commerce, and in other relevant sectors. The Digital Economy of India is expected to grow from the current figure of $270 billion to around $1 trillion in the next 5–7 years[1].

In a digitally connected society, individuals are constantly disclosing their identity and also generating valuable data, which can be used to track their behavior, choices and preferences. The user data is generated not just by active sharing of information, but also in a passive manner including by way of accessing the content world and being connected on the internet. With every click on the Internet, individuals are sharing their personal information and data at multiple levels. As we move towards a Digital Economy and increase our reliance on Internet-based services, deeper and deeper digital footprints are being created and personal information is becoming available in the public domain. The lines between the personal and public domain are blurring and beginning to merge. **Therefore, it is imperative to establish an effective, robust and stringent regime for privacy and security of customer information and data including storage and use of the data. Such a regime is crucial for building confidence and trust amongst users for wider adoption of Internet-based services and doing business in India**.

The issue of privacy and security of personal data is not just limited to the entities in the telecommunication sector. This issue is, in fact, critical for all sectors and the various services. For example, any customer who shares his/her personal information with the Telecom Service Providers (TSPs) or with banks, financial institutions or any other commercial entity, expects the same level of protection to be provided for his/her information. In the Internet services sector, TSPs, Over-the-Top (OTT) communication

[1]http://economictimes.indiatimes.com/news/economy/indicators/digital-economy-can-reach-4-trillion-in-4-years-tech-sector-to-government/articleshow/59188885.cms

service providers, content providers, equipment/handset manufacturers, entities dealing with Smartphone operating systems, and browsers, etc. operate in the same Internet ecosystem. In this sector, customer privacy has three significant sources of vulnerabilities—device, network and content providers—and any law that limits its scope to TSPs alone will not be able to holistically address the issue of protection and privacy of personal data.

**Therefore, we are of the view that the data protection rules should be uniform and must involve all stakeholders operating within the Internet ecosystem irrespective of technology and services being provided by them.** Further, **a Principle-based Horizontal Rule** on data privacy and protection that applies to all the entities and individuals who collect, store and process the customer data is the essential requirement and best way forward. Such rules should also be aligned with the international best practices and data protection laws that exist in the more developed parts of the world.

The new framework should unlock the data economy and therefore, should establish the distinction between the `Personal Information' and `Aggregate or anonymized data'. This distinction will help in realizing various benefits, which can be derived by performing 'Big data analytics' on such aggregate data which helps in understanding user preferences and to develop innovative and customer friendly products and services.

While the current Consultation Paper of the Authority is limited to the Privacy, Security and Ownership of the Data in the Telecom Sector, the Authority is also requested to be cognizant to the current law(s) on data privacy as are currently and also any amendments thereto and evolution of the same in the future. As we understand, the Government is contemplating amendments to the existing law and also planning to promulgate new laws in the near future. The Supreme Court of India is also seized of several matters which have challenged and questioned the right of the various authorities to seek and maintain the personal data of the citizens. At an overall level, the regime and conditions that are proposed to be imposed by the TRAI ought to be in complete harmony with the same.

In the above context, we hereby put forth our views on the questions raised by the Authority in this Consultation Paper.

**Issues for Consultation:**

**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?**

**Airtel's Response:**

1. We believe that the provisions embedded in the telecom licence agreement related to privacy of customers and data protection are quite robust and apt, including that the TSPs are subjected to stringent financial penalties if there is any failure to comply with the same. Therefore, we do not suggest any change in these provisions for TSPs.

2. However, the same rules are not applicable to other entities, such as, OTT communication service providers, content providers, device manufacturers, browsers, operating system providers, etc. herein called as "Other Players" operating in the Internet ecosystem. TSPs and the other players operating in the same Internet ecosystem and dealing with same personal data are governed by different rules and regulations. For example, while TSPs are not allowed to send the personal data of their customers outside India, there is no such prohibition/restriction on other players. In fact, in most cases, the personal data being handled by these players resides outside of India.

   As yet another instance of this issue, various applications and mobile operating systems capture a lot of customer data without providing full understanding to their customers regarding how their data will be used (for example, to "sell" to third parties or be used indirectly for advertising, etc.).

3. The current laws and regulations do not comprehensively safeguard the personal data of individuals. **Therefore, the rules on privacy of customer data and its protection require a holistic review and should be uniformly applicable to all the players (both TSPs and other players) operating in the Internet ecosystem. Any law pertaining to data protection should govern all the entities and individuals that collect and process the customer data irrespective of the technology and service being provided. A principle-based horizontal data protection law, in line with international best practices, will be the right approach to promote Digital Economy and Internet-based services. Such law will ensure non-discrimination and also become applicable to entities beyond the telecom sector.**

**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?**

**Airtel's Response:**

1. The definition of 'Personal Information' promulgated in the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 is;

   ***"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.*

2. We submit that the above definition is appropriate and does not require any modification.

3. Further, any law related to customer privacy and data protection should recognize different types of information/data being handled by various entities, as stated below:

   a) **Personal Information:** Information collected by an entity/ individual that identifies a person as a user. Such information is required for the provision of services by that entity/individual and/or is required to be maintained under the legal/regulatory framework.
   b) **Non-Personal Information or Anonymous Information:** Information about the person who is a user, which cannot be used to identify that person. Such Anonymous Information will be used to improve various business processes, develop innovative products, measure effectiveness, and customize content and offerings to the said customer.
   c) **Aggregate Information:** Combining anonymous information into groups which can be used by an entity for analytics, customized communication, content, offers, etc.

4. Therefore, any privacy and data protection law should acknowledge a distinction between the `Personal Information or Personally Identifiable Information (PII)' and `anonymized or aggregate data'. While sharing or using PII should be done only with the explicit consent of the customer, any other information, whether anonymized or aggregate, should be allowed to be shared on overarching consent for the usage of services.

5. We also believe that the process of explicit consent should be clear and unambiguous. Further, the privacy rules of any legal entity whose services are being offered and used within the jurisdiction of a country (India, for example) should comply with the privacy rules of that country.

6. It will become increasingly important in this age of 'big data analytics' and IoT to have the explicit recognition that anonymous data is not personal data and that pseudonymisation[2] can provide genuine safeguards without the need for explicit consent of the customer.

7. To safeguard the interest of consumers, there should also be a mechanism wherein the consumers can gain control on the use of their personal information, either commercially or otherwise. There should be an application or functionality through which consumers can keep track of all their previous consents given for specific end use and also manage the "opt-in" or "opt-out" option given for sharing of their personal data.

8. Further, the customer should have the right to be forgotten by seeking the deletion of all the information (including online activities), which an entity/individual has stored, other than the ones that are necessary for providing the services by that entity and the information that is mandatory to be stored due to legal/regulatory reasons. Even that should be the choice of the customer as to stop the services and choose to have his/her data deleted completely. The entities should not store and use the personal information of their customers once they stop using the services/products of that entity, beyond the mandated period under the law, if any.

[2]Pseudonymisation takes the most identifying fields within a database and replaces them with artificial identifiers, or pseudonyms. For example a name is replaced with a unique number.

**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.**

**Airtel's Response:**

1. We believe that the responsibility of Data Controllers should be similar to the entities dealing with the processing and collecting of the customers' data. The Data Controller should not have any rights to supersede the rights of the customer.

2. The best way to regulate Data Controllers is to set out the principles which they are expected to uphold and to encourage them to adopt comprehensive internal security programs. They should be able to demonstrate the compliance to consumers and the Government with their policy guidelines.

3. The Data Controllers should be restricted from on-selling the consolidated data either anonymous or otherwise.

**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 set up 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?**

**Airtel's Response:**

1. We believe that fears relating to the abuse of data can be mitigated by stringent law followed by best practices by all entities dealing with customer data. All entities that collect and process the customer data/information should disclose any breach or leakage of any information related to their customers to the appropriate legal/regulatory authorities. All the personal information should be kept anonymous or encrypted in line with the industry standards. All entities should have access controls that prevent the access of customer information or personal information to

their employees, affiliates or partners and that the same is made available to them only for specific purposes, which aid them in providing the services subscribed by the customer. All parties, including third parties should be subjected to the same information security guidelines as applicable to the entities while they are collecting the information about the customers.

2. Further, an adoption of audit entailing the mix of a technology-enabled architecture and human intervention to track the use of personal data and other information would be an appropriate approach. The technology-based architecture can be used for checking consent logs and its specific use, as it is used in the present VAS-related audit. Human intervention is required for checking the manner or spirit in which the data privacy policy is followed by the Company.

3. The compliance to privacy and data protection law can be assessed by the companies themselves or by third parties such as the accredited standard bodies like ISO for security; or by auditing firms that have the requisite expertise and capability. The Government and the Regulators should also supervise the compliance of all entities dealing with personal data and may also conduct audits on a case-to-case basis at regular intervals.

**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?**

**Airtel's Response:**

1. While the protection of Personally Identifiable Information is critical; the usage of data in an aggregate or anonymous manner is also equally critical for improving services, developing innovative products, and for social and economic welfare. While the Government should encourage the creation of new data-based businesses, it should also implement programmes and take measures to build the trust of individuals whose data is being collected by various entities.

2. **Therefore, the data protection rules should be uniform and must involve all stakeholders, irrespective of the technology/service they provide or the sectors they operate in. Such rules should be aligned with international best practices to safeguard the consumer interest and to accelerate the Digital Economy of the country.**

**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?**

**Airtel's Response:**

1. We believe that there should not be any centralized body of Government to set up a data sandbox, which allows regulated companies to create anonymous data sets. This central body may work as a road block to an emerging dynamic business model.

2. The Government should restrict itself in only providing the guidelines/laws on the creation and sharing of anonymized data sets for developing new Digital Services and enhance the Digital Economy, which should be applicable for all entities uniformly.

3. We recommend that sharing of aggregate or anonymized data should be left to the commercial needs of corporate bodies, which would be under the purview of a uniform law.

**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?**

**Airtel's Response:**

1. We recommend that there should be some security measures that apply horizontally to all stakeholders, which can work as a general standard for ensuring data security. Further, the Government may consider limiting certain data (such as biometric data, or data related to critical infrastructure) to remain within the country to protect national security and safeguard the public interest.

2. Data security breaches are becoming commonplace due to server issues, poor security practices, human error and unwanted threat/hacking. The hackers may target individuals by leading them to a phishing site and gain access to their credentials. This would provide hacker with the resources required to gain access to customer information, which the entity possesses. In such cases of security breaches, agencies like National Computer Emergency Response Teams can work with all stakeholders the way other agencies such as Disaster Management works. Further, to prevent leakages and to minimize impact, personal consumer data should always be

encrypted and overall information should always be stored without directly usable PII.

3. The Government has mandated effective security norms and regulations for securing the Telecommunication infrastructure, these should be extended to cover the infrastructure of the core digital ecosystem as well.

**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?**

**Airtel's Response:**

1. The Internet services sector is not limited to TSPs/ISPs alone; it includes content providers, equipment/handset manufacturers, OTT players, entities dealing with Smartphone operating systems, browsers, cloud service providers, caching and Content Delivery Network (CDN) providers, etc. We strongly believe that each stakeholder operating in the Internet service sector should be subjected to the same rules to ensure that all entities are treated equally and that the customer is not at a disadvantage in any stage. For example, while TSPs are forbidden from sending customer data outside India, other entities, such as browsers, applications, mobile Operating System (OS) and handset Original Equipment Manufacturers (OEMs) are not.

2. Further, it[3] is the individuals' rights and expectations that they are provided with the same level of protection for all functionally equivalent services, irrespective of whether they are provided by traditional telephone companies, by Voice-over IP (VoIP) services, or via mobile phone voice and OTT messaging applications. This is because the users' expectations are often similar with respect to privacy and confidentiality of their communications and any breach of confidentiality may be equally intrusive and violative of the fundamental right to privacy. For users, it is possible to begin a conversation using the messaging function of a game, then move to an OTT instant messaging service, exchange mobile SMS' and eventually launch a call between two phones. All these different types of communications may be performed by using the same device, i.e., Smartphones, and for the user, different

[3] https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf

legal frameworks for the services used are by no means evident, understandable or even controllable.

3. Therefore, the rules related to data protection should be uniformly applied on all the stakeholders operating in the Internet ecosystem.

**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?**

**Airtel's Response:**

1. OTT communication service providers are offering many services that are equivalent to telecommunication services like voice telephony or messaging which should only be provided by licensed telecom service providers. Therefore, there should be the principle of 'Same Service, Same Rule', so that rules are applied uniformly including issues related to data protection on TSPs and OTT Communication Service Providers.
2. **Thus, in our view the data protection rules should be uniform and must involve all the stakeholders operating in the Internet ecosystem irrespective of the technology and service. A Principle-based Horizontal Rule** on data privacy and protection that applies to all the entities and individuals who collect, store and process the customer data and these rules to be aligned with international best practices, is the best approach.

**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?**

**Airtel's Response:**

1. Currently, all telecom operators are subjected to the security guidelines which govern lawful interception by the designated security agencies. Further, the telecom operators are also required to share the information related to their customers with these agencies. These security guidelines have evolved over a period of time-based on market and technological changes. However, the same rules are not applicable on

other stakeholders (Other players) operating in the Internet ecosystem, which provide communication-related services.

2. For example, OTT Communication Service Providers offer calls across telecom networks in India using strong encryption and their switching servers being located outside the country. This effectively prevents any lawful interception and/or monitoring of calls handled in their switching servers/network. These players also avoid sharing subscription details of customers and/or logs of communications to the security agencies. In fact, some OTT Communication Service Providers facilitate spoofing of Calling Line Identification, which makes it difficult to identify or locate the actual caller.

3. **Therefore, we believe that the rules related to national security should be applied uniformly on all stakeholders operating in the Internet ecosystem.**

**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?**

**Airtel's Response:**

1. In this era of globalization, the flow of cross-border data is essential to promote international trade and to support new business models; however, the same raises concerns about privacy and create new challenges to the entities with respect to protecting individuals' personal information and to meet national security requirements.

2. We believe that principally, there should not be any distinction over the accountability of the concerned stakeholders if the data is flowing within the country or outside the country. Entities sending the consumer data abroad should continue to remain liable under Indian law for action taken by the foreign handler of this data as they would have remained liable for Indian entities in similar situations. Further, the foreign entity handling the data should also be subjected to Indian laws related to privacy and data protection.

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

Moreover, the rules related to any entity providing communication- related services should be the same irrespective of the technology and platform. For example, TSPs are not permitted to send their user data outside India, whereas there is no such restriction on other players dealing with the same data.

4. The cross-border flow of data requires extensive cooperation at the global level and the related issues (jurisdictional) in the digital ecosystem should be addressed through bilateral agreements between the Government and other global associations such as the United Nations Organization (UNO).