November 6, 2017

Shri Arvind Kumar,
Advisor (BB&PA),
Telecom Regulatory Authority of India
Mahanagar Doorsanchar Bhawan,
Jawahar Lal Nehru Marg, Old Minto Road,
New Delhi - 110 002

Subject: **Vodafone's Response to TRAI Consultation Paper dated 09th August 2017 on "Privacy, Security and Ownership of the Data in the Telecom Sector"**

Dear Sir,

This is in reference to the Consultation Paper on "Privacy, Security and Ownership of the Data in the Telecom Sector", issued by TRAI on 09.08.2017.

In this regard, please find enclosed our comments to the above-said Consultation Paper.

We hope that our submissions will merit your kind consideration and support.

Thanking you,

Yours sincerely,

For **Vodafone India Limited and**
Vodafone Mobile Services Limited

P. Balaji
Director – Regulatory, External Affairs & CSR

Encl: As stated above

Vodafone Response to TRAI Consultation Paper dated 9 August 2017 on Privacy, Security and Ownership of the Data in the Telecom Sector

Background to the Consultation

We understand that the aim of the Consultation Paper is to identify the key issues pertaining to data protection in relation to the delivery of digital services. This includes the provision of telecom and Internet services by telecom and Internet service providers (TSPs) as well the other devices, networks and applications that connect with users through the services offered by TSPs and collect and control user data in that process.

As more services use mobile and communications related data for an ever-expanding range of uses, customers need to be able to understand and be able to control how information about them is used. Smartphones, tablets, e-readers, apps and new technologies using the 'internet of things' (such as connected cars, smart grids and mHealth) offer many economic and social benefits, but also raise some complex privacy issues. For example, mHealth services may enable physicians to monitor patients round the clock by having remote access to their health devices and data, but by doing so sensitive health data may need to be transmitted across communications networks, hosted in the cloud, and processed by a range of applications used by medical staff.

Governments also have legal powers to demand access to customer communications and data.

At the outset we say that Vodafone is committed to protecting the information and respecting the privacy of our customers. The way we handle privacy and security is a vital part of our responsibility to our customers and essential to the success of our business.

The confidentiality of customers' personal and private communications is a fundamentally important requirement for any communications company as the company will manage a great deal of sensitive information including customers' personal communications, their location and how they use the internet.

To ensure customers' privacy, the security of their information and communications is to be ensured first. This includes areas of how to securely create, use, store or dispose of all information, so that it cannot be lost, stolen or manipulated, or used without proper authorization.

Personal data also has enormous potential to create economic and social value, both for the individuals concerned and for the businesses who serve them. In order to ensure this opportunity is executed well, we have to use technology to make it easier and more intuitive for customers to take control of how their data is used. Many of the latest developments in the ICT sector raise privacy and security issues, concerns and opportunities. These include 'big data' analytics, connected cars, smart cities, smart metering, mHealth, Mobile payments and Smart working.

However, the TRAI is aware that privacy concerns also emanate from the activities of a variety of other stakeholders that process and control the personal data of users. This includes stakeholders like content and application service providers, device manufacturers, browsers, operating systems, etc. It is submitted that these do not fall within the jurisdiction of TRAI and TRAI does not, in the consultation deal with how the issue of equivalence of rules will be addressed.

We also note that there are a host of other laws, acts in the country, that have provisions related to privacy, confidentiality and data protection.

We further note that a High Powered Committee has been set up under the directions of the Hon'ble Supreme Court, to lay down a data protection framework. We thus believe that the recommendations of the TRAI, will serve as an input to the above Committee in laying down a data protection framework that is applicable to all entities that have access to the data of the subscribers/consumers.

Insofar as the TSPs are concerned, TRAI is aware that the TSPs already have very rigorous privacy security and data protection requirements that are applicable to them under their licenses. These specific provisions are in additional to the general provisions that are prescribed under the Information Technology Act, 2000, which is also be applicable to the TSPs. There are certain inconsistencies /anomalies between the provisions of license and the provisions of the Information Technology Act, which leads to confusion for the TSPs with regard to which provision is applicable and also hampers them in the provision of service.

For level playing field, it is desirable that the specific provisions under license are dropped and only the IT Act is applicable to them as all to the other players in the digital ecosystem.

Against the above backdrop, we submit our responses to the issues raised for consultation.

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?

a) As mentioned in TRAI's consultation paper, privacy concerns emanate from variety of players in the eco-system. The telecom subscriber's information like device number, location, mobile number, name etc. while it is being kept confidential by telecom operator but due to use of

various applications, device fingerprinting, operating systems for devices, browsers, operating systems etc. the same information is available to other players in the eco system.

b) The telecom subscribers, thus face different levels of data protection qua different elements in the supply chain, which does not adequately safeguard their interests.

c) There are different privacy and data protection requirements that are applicable to different players – creating non-level playing field.

d) The privacy and data protection requirements need to be the same for all players in the eco system.

e) For example, we have repeatedly being representing to the TRAI with regard to the non-level playing field especially between the OTT Communication and telecom players on the issues of security, privacy, data protection, etc. This differential requirements may provide an undue advantage to OTT Communication players as also the other digital/internet players that too at the cost of telecom subscribers.

f) In the interest of telecom subscribers, there should be transparency and uniformity of process for them to exercise choice. In this respect the governing rules should be same.

g) As pointed out, the IT Act is applicable to all, including TSPs and contain provisions with respect to privacy as well as security of data. It may be in the interest of telecom subscriber that for better transparency, uniformity in process to exercise any choice, reliability, balance, accountability a uniform set of requirements be applicable to all players in the eco-system, including telecom service providers. Therefore, only the provisions of the IT Act be applicable to all.

h) In the event that any further changes are required in the IT Act, these would in any event be applicable to all players.

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?

a) The IT Act defines information, personal information and Sensitive personal information separately as given below

- "**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)
- "**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.
- "**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 definition of personal data as well as sensitive personal data given in the IT Act 2000 are sufficient and should be continued with.

c) Personal data /information has been defined under the IT Act as information that is capable of identifying such person.

d) Any data protection regulation /requirement in terms of consent, opt-out, etc., should confine itself only to personal data/sensitive personal data of an individual that identifies the said individual.

e) Users consent may be taken before the same is shared in a user identifiable format with any third party for commercial purposes.

f) Anonymized usage of data should not come under the purview of any regulation as data analytics is a growing field with immense socio-economic benefits.

g) TRAI has also noted in its consultation paper that traditionally the scope of data protection regulation world over has been limited to personal data.

h) It may be prescribed that every company, entity, digital player is required to place its Data Protection, Security and Privacy Policy in the public domain/on its website. The Policy may describe the type of information collected, the purpose of use of the information, to whom or how the information can be disclosed and the reasonable security practices and procedures followed to safeguard the information.

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.

a) A Data Controller should take responsibility of how it collects, uses and manage customers' information – from ensuring the confidentiality of their personal communications and respecting their permissions and preferences, to protecting and securing their information.

b) The role of data controller needs also to be seen from point of view of advancement of technology. For example, in case of IOT a data controller will be the person who writes the code for the applications that run the machine.

c) The Data Controller should normally be free to use the information available with it, in an anonymized format for data analytics for innovative products and services. There should be no restriction placed on the use of such metadata as the same does not in any way identify the individual consumer, but uses the trends, behaviours, etc for market analytics, innovative services, creation of new businesses, etc.

d) It is reiterated that personal data as defined under the IT Act is user identifiable data. Such behavior may be required to be shared by the Data Controller in certain circumstances, which could include security requirements.

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?

a) We submit that it would be desirable to lay down good practices which could include publishing of the Data Protection, Security and Privacy Policy in the public domain/on the website.

b) Further, it may also be required that all data collection & processing entities should obtain certification of their IT systems viz; International Standard IS/ISO/IEC 27001 (for Information Technology - Security Techniques - Information Security Management System)

c) We support the development of an Electronic consent framework, but believe that an audit based approach may not be required / desirable at this stage.

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?

a) India is adopting digitization rapidly and various Government programs focuses on citizen centric services through use of data analytics. In fact, the theme of this year's World Communication & Information Society Day was 'Big Data for Big Impact". Big data and Analytics allows people to make decisions based on patterns and relationships and the possible benefits of Big Data Analytics in Government could range from transforming government programs an empowering citizens to improving transparency and enabling the participation of all stakeholders.

b) Data analytics can help Government /Economy in better social good and mechanisms for better disaster management and in many other areas such as:
   i. Solving traffic problems in cities, resolving traffic congestion, smart parking,
   ii. Targeting healthcare delivery, controlling disease spread,
   iii. Efficient supply chain management
   iv. Preventive steps for environmental protection
   v. Providing a personalized educational experience for students,
   vi. Enabling securing to individuals and society at large, and
   vii. Informed policy making

c) We are gratified that TRAI has rightly recognized the potential of new data based businesses; these includes Big Data, Analytics, Data Mining, etc. and we agree that these must be encouraged/facilitated.

d) We are of the view that Authority must recommend the key principles based on which various types of data can be used /shared.

e) As submitted above, data can be classified into personal data, sensitive personal data and meta data [which is aggregated/anonymized use based on specific attributes] The approach to data protections needs to be different in all cases, with use of meta data being freely permitted. Protection standards need to be laid down for personal data [user identifiable] and especially in case of sensitive personal data.

f) We once again reiterate that Privacy, Security and Data protection rules, should not be sector specific, they should be applied horizontally across all sectors.

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?

a) Firstly, we submit that all companies /players handling data should be treated equally and the rules cannot be different for regulated /unregulated companies. Data cannot require protection only in the hands of a 'regulated' company as this would defeat the entire objective of the exercise.

b) We believe that the data available to a Data Controller by virtue of the service provided by it, cannot and should not be required to be shared with any third parties either by way of a sand box or anonymized data sets. Any requirement to share such data sets will hamper innovation.

c) We believe that instead of companies, if such a data sandbox requirement is put on government data, this will greatly facilitate innovation and new businesses. This may be considered by TRAI.

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?

a) We believe that it is desirable to adopt a principles based approach for the present.

b) As suggested above, requirement for publishing of a Data Protection, Security and Privacy Policy in the public domain/on its website, should be prescribed. The Policy may describe the type of information collected, the purpose of use of the information, to whom or how the information can be disclosed and the reasonable security practices and procedures followed to safeguard the information.

c) A technology based solution may be developed to address specific concerns that may arise.

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?

a) It may first be noted that as far as we are aware, no security breaches have taken place on GSM based systems, which is testimony to the robustness of these networks.

b) There is also a process that has been put in place to share information amongst stakeholders with regard to cyber-attacks, this has also helped in strengthening and preserving the safety and security of telecommunications infrastructure; however, such process may be extended to include all stakeholders.

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?

a) TRAI has recorded in its consultation that apart from the services provided by TSPs, it is well recognized that privacy concerns also emanate from the activities of a variety of other

stakeholders that process and control the personal data of users. This includes stakeholders like content and application service providers, device manufacturers, browsers, operating systems, etc.

b) TRAI is also aware that there is no parity in the data protection requirements and that different rules apply to different players. There must be level playing field for all.

c) Further, the rules should not be over restrictive – they must balance the customer's privacy and data protection requirements with the need to facilitate innovative technology based solutions.

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?

a) Yes.

b) TRAI is aware that there is no parity in data protection norms between Licensees vis-à-vis non-license entities. In addition to specific license provisions on privacy, Security and Data Protection, IT Act also applies to licensees. In absence of this parity, there is lot of confusion for Licensees as it places them in disadvantageous position in offering many data based services in competition with non-licensed entities/OTT players.

c) Privacy, Security and Data Protection rules must be the same for all. This may be done through the IT Act, with further amendments, if required and by way of a separate Privacy, Security and Data Protection law.

d) Specific license provisions on Privacy, Data security and protection may be removed from license & only IT Act provisions may apply.

e) Any changes contemplated in the IT act to further strengthen Privacy, Data security and protection, would be applicable to all players.

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?

a) Meta data or anonymized data should not be subject to any data protection requirements.

b) As submitted above, data protection requirements should be applied only in respect of user identifiable information and sensitive personal information.

c) It may be noted that Rule 6 **on Disclosure of information,** Information Technology (Reasonable Security Practices and Procedures and Sensitive Data and Personal Information) Rules, 2011 permits disclosures if such disclosure has been agreed to between parties, where the disclosure is necessary for compliance of a legal obligation, sharing with Government agencies mandated under the law to obtain information or by Order under law. The relevant Rule is extracted below, for ready reference.

6. Disclosure of information.— (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, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation: Provided that the information shall be shared, without obtaining prior consent from provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. The Government agency shall send a request in writing to the body corporate possessing the sensitive personal data or information stating clearly the purpose of seeking such information. The Government agency shall also state that the information so obtained shall not be published or shared with any other person.

(2) Notwithstanding anything contain in sub-rule (1), any sensitive personal data on Information shall be disclosed to any third party by an order under the law for the time being in force.

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?

a) TRAI is aware that boundaries for data travel/storage has blurred and almost everyone now has his Personal Information stored in global social / financial sites such as Gmail/Yahoo/Visa/Master Card etc.

b) Any restriction on cross border flows is archaic in the era of globalization and Cloud computing. Information must be allowed to freely flow across borders. The Data controllers must be responsible to ensure that the data is assured of the same level of protection that is applicable in their own country.

c) The need of the hour is for collaborative regulations for digital societies where boundaries are fast vanishing and loosing relevance. Economies are increasingly moving towards digital adoption for sustainability and in this sequence innovations will always outplace regulations and thus light touch regulations helps a flourishing economy by embracing innovations.

d) It may be noted that the IT Act permits cross border flows even in case of Sensitive Data and Personal Information. Rule **7 on Transfer of information,** Information Technology (Reasonable Security Practices and Procedures and Sensitive Data and Personal Information) Rules, 2011 **is extracted below, for ready reference**

7. Transfer of information.-A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

e) As regards jurisdictional challenges, we note that the TRAI in its recent recommendations on Cloud Services has recommended that:

"*4.4 To address the issue of access to data, hosted by CSPs in different jurisdictions, by law enforcement agencies:*
a. Robust MLATs should be drawn up with jurisdictions where CSPs usually host their services, enabling access to data by law enforcement agencies
b. Existing MLATs should be amended to include provisions for lawful interception or access to data on the cloud."

f) A similar approach may be recommended in respect of jurisdictional challenges pertaining to cross border flow of information in the digital ecosystem.

New Delhi
6 November 2017