6th November 2017

Mr. Arvind Kumar
Advisor (BB&PA)
Telecom Regulatory Authority of India
Mahanagar Doorsanchar Bhawan
Jawahar Lal Nehru Marg
(Old Minto Road)
New Delhi – 110002

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

Dear Sir,

This is in reference to your Consultation Paper number 09/2017 dated 9th August 2017 on **"Privacy, Security and Ownership of the Data in the Telecom Sector".**

As desired, we hereby enclose our response to the questions raised in your above mentioned Consultation Paper. We hope our response will be given due consideration. We shall be obliged to address any further queries from your good office in this regard.

Thanking you and assuring you of our best attention always.

Yours sincerely,

Satya Yadav
Addl. Vice President – Corporate Regulatory Affairs
Tata Teleservices Limited
And
Authorized Signatory
For Tata Teleservices (Maharashtra) Limited

Encl: As above

TTL response to Consultation Paper on "Privacy, Security and Ownership of the Data in the Telecom Sector"

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

TTL Response:

Rapid evolution of telecommunication services in India has enabled better connectivity among users along with multi-fold increase in the use of information and communication technology services. A quantum leap has been witnessed in India over last 2 years, on data collection, storage and analytics have therefore become a widely used tool for business to monetise their products and services in order to gain a competitive advantage over competition.

Currently Telecom Service Providers are covered under provisions relating to the protection of consumer's data under Indian Telegraph Act 1885. Clause of Unified License agreement also put Licensee under an obligation to ensure protection of privacy of communication and ensure that unauthorized interception of messages do not take place. Directions have also been issued by TRAI in Feb 2010, directing TSPs to ensure compliance of licensing conditions regarding confidentiality of information of subscribers and privacy of communications. In order to ensure that the customers are protected from phishing attacks, NCPR (National Customer Preference Register) was created by TRAI, which prohibits companies making unsolicited commercial communication with customers, registered in NCPR.

TSPs are also covered under Information Technology Act 2000, that contains provisions relating to protection of data and interception of information by authorized agencies.

In view of the above, we are of the opinion that the data protection requirements currently applicable to telecom players in the eco-system in India are sufficient to protect the privacy, confidentiality and security of telecom subscribers, however, we feel that the foreign companies establishing their business in India dealing into content and application service, Device manufactures, Browsers, operating system etc, that connects with users through the services provided by the TSPs must ensure that their local entities adheres to Indian Data Protection and Data Privacy law requirement, even if these local entities are following global best practices.

Question 2: In light of recent advances in technology, what changes, if any, are recommended to the definition of personal data? Should the User's consent be taken before sharing his/her personal data for commercial purposes? What are the measures

that should be considered in order to empower users to own and take control of his/her personal data? In particular, what are the new capabilities that must be granted to consumers over the use of their Personal data?

TTL Response:

As per the Information Technology Act 2000 (21 of 2000) and Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Personal Information means "Any information that relates to natural person, which either directly or indirectly, in combination of other information available or likely to be available with a body corporate, is capable of identifying such person." Sensitive personal Data or information of a person means such information which consists of information related to Passwords, Financial information such as Bank Account or Credit Card or Debit Card or other payment instrument details, Physical, physiological and mental health condition, Sexual orientation, Medical records and history, Biometric information, Any detail relating to the above clauses are provided to body corporate for providing services and Any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise. The definition covers all aspect of personal data and may not require changes currently.

India is taking a giant leap towards digitization. There is an unprecedented amount of data pool available with the Government and Private Sector players and this pool has been growing rapidly. Adoption of Social networking Web-sites, Applications have enabled publically sharing of personal information, political & religious views, Geo location, which may pose a great risk to the subscriber, in lieu of understanding the long term implication of sharing this information. The data is also being collected by various websites, e-banking, e-commerce, search engines, applications etc through user's action, with OR without their knowledge. This data is then correlated using more advanced analytical tool to generate economic value out of the data like creation of new demands, and build relationships for generating revenue from their services. The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 have defined the Sensitive Personal Data expect for the information freely available or accessible in public domain. Considering that the sensitive personal information such as political opinion, religious views etc, if processed and shared for commercial purpose, may be misused and may also have an adverse impact on the user. We hereby recommend, incorporating a category of sensitive personal data which covers Racial or Origin, Political opinions, Philosophical or religious beliefs, Offences committed to OR alleged to have committed, Prosecution taken, convictions obtained and punishment imposed. Processing or sharing of such personal data for commercial or non-commercial purpose should be done only on the following grounds:

- Explicit consent of subscriber.
- Specific obligations under law.

The private sector and the civil society needs to build legal regimes and practices that are transparent which inspires trust and enhance their ability to control the access of their data. In order to empower subscribers and give them full control of their personal information, it is suggested that the subscribers should be given the right to withdraw their consent for collecting, processing and sharing of their personal data, unconditionally, unless it falls under lawful obligation of the data controller.

Question 3: What should be the Rights and Responsibilities of the Data Controllers? Can the Rights of Data Controller supersede the Rights of an Individual over his/her Personal Data? Suggest a mechanism for regulating and governing the Data Controllers.

TTL Response:

A report by the group of experts on privacy, constituted by the planning commission, headed by (Retd.) Justice A.P. Shah, Former Chief Justice, Delhi High Court, in October 2012, have given their recommendations in their report stating that a set of National Privacy Principles can be enumerated as the distillation of global best practices, followed by US, OECD, EU and APEC, can be effectively implemented in Indian conditions. These privacy principles shall also cover the rights and responsibilities of the Data Controllers as listed below:

1. The data controller should give simple to understand and notice to the user in a transparent manner, which should include:
    a. What personal information is being collected?
    b. Purpose of collecting this information
    c. Use of collected information
    d. User's explicit consent to share this information to third persons.
    e. Security and safeguards established with regards to the collected data/ information.
    f. Process available to the user to access and correct their own personal information.
    g. Contact details of the privacy officers for filing a complaint
2. The data controller should collect and process personal information of the user only which is necessary for the purpose identified for this collection.
3. The data controller shall be accountable for complying the measures which give effect to the privacy principles. Such measures should include mechanism to implement privacy policies, including training and education, audits etc.

Implementation of the above recommendation of Planning Commission report clearly defines the rights and responsibilities of the data controllers, effectively protecting the privacy of the users. Considering that the data collected by the Data Controller is the

personal data of the user, hence the user or the individual rights shall always supersedes the rights of data controller.

TTL is of the view that the data controllers may be regulated and governed by implementing a Co-Regulatory Enforcement Regime, as recommended in the planning commission report, Oct 2012. The report recommends to establishment an office of the Privacy Commissioner, both at the central and regional levels. The Privacy Commissioners shall be the primary authority for enforcement of the provisions of the Act. A system of co-regulation, with equal emphasis on Self-Regulating Organisations (SROs) being vested with the responsibility of autonomously ensuring compliance with the Act, subject to regular oversight by the Privacy Commissioners. The SROs, apart from possessing industry-specific knowledge, will also be better placed to create awareness about the right to privacy and explaining the sensitivities of privacy protection both within industry as well as to the public in respective sectors. This recommendation of a co-regulatory regime will not derogate from the powers of courts which will be available as a forum of last resort in case of persistent and unresolved violations of the Privacy Act.

Question 4: Given the fears related to abuse of this data, is it advisable to create a technology enabled architecture to audit the use of personal data, and associated consent? Will an audit-based mechanism provide sufficient visibility for the government or its authorized authority to prevent harm? Can the industry create a sufficiently capable workforce of auditors who can take on these responsibilities?

TTL Response:

As mentioned in our response to Q1, Telecom Service Providers are covered under provisions relating to the protection of consumer's data under Indian Telegraph Act 1885. Clause of Unified License agreement also put Licensee under an obligation to ensure protection of privacy of communication and ensure that unauthorized interception of messages do not take place. In order to ensure that customers are protected from phishing attacks, NCPR (National Customer Preference Register) was created by TRAI, which prohibits companies making unsolicited commercial communication with customers, registered in NCPR. Hence, TTL is of the view that TSPs in the country have already put in place adequate security measures to protect their network and data privacy of their customers. There is no requirement to create technology enabled architecture to audit personal data and associated content for TSPs.

We also wish to highlight that putting technology controls in place by entities to regulate some processes would still require human intervention as there will be instances where hardcore computer logics would not work and yield desired results. Hence creating a technology enabled architecture to audit the use of personal data and associated content is a vast subject and requires debate involving, OTTs, application providers, browsers, operating systems, online payment web sites, banking websites, e-commerce websites and

other stakeholders in the digital ecosystem to study and understand if such an architecture is implementable/ executable and auditable, for the government or it's authorized authority.

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

TTL Response:

No Comments

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

TTL Response:

Internet penetration has been growing in India at a rapid speed. Studies have also indicated that the growth of App usage in India has been 43% in last 4 years against the global growth at 11%. While the use of these Apps brings many efficiencies and benefits to both users and the developers they also pose several concerns from data security perspective as these Apps collects lot of personal information of the customer from their devices including metadata. Transfer of personal information is a risk because of the open architecture of the Internet. According to MetaIntell, today 92% of such internet/ OTT applications uses non-secure communication protocols.

Mobile applications can extract user information from the devices and this information is used for carrying out marketing activities. The applications also can extract sensitive information like Banking Details, Passwords, photographs etc of the user. The always online state of Mobile phone devices exposes users to cybercrime as most of the apps can trace the Geo-location of the user. This raises concerns on privacy and security of an individual.

In view of the above, TTL is of the view that government mandated data sandbox may choke off investments and innovation incentives and thereby harm consumers, particularly in light of the emerging and dynamic nature of business models and technologies related to anonymised data. Hence Also, haring anonymized data sets with Government authorized regulated companies carries concern, which may impact the intellectual property and trade secrets. Hence, we recommend data portability may be allowed and regulated within the National Privacy Policy Principles.

Question 7: How can the government or its authorized authority setup a technology solution that can assist it in monitoring the ecosystem for compliance? What are the

attributes of such a solution that allow the regulations to keep pace with a changing technology ecosystem?

AND

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

TTL Response:

We believe that that no technology exists where security is unbreakable, however, instances of security breach and attacks on GSM networks are not common, as such attacks on GSM network requires specialised equipments, computers and resources which are beyond the capabilities of most of the people and organisations. Also Section 70 of the IT Act provides for the declaration of certain areas as critical information infrastructure (CII) and the need for introducing appropriate measures for the security of these systems. Keeping in view the critical rule of the telecommunications sector, the National Critical Information Infrastructure Protection Centre (NCIIPC), has designated telecommunication to be one of the CIIs. Also TSPs in India are covered under provisions relating to the protection of consumer's data under Indian Telegraph Act 1885 and clause of Unified License agreement also put Licensee under an obligation to ensure protection of privacy of communication and ensure that unauthorized interception of messages do not take place. TSPs, in order to safeguard their operations and business interests have deployed adequate security measures to ensure that their critical infrastructure and customer data is safe and TSPs are able to meet their license obligations and obligations to the customers and public.

However, TTL will be pleased to extend it's unconditional support on introduction of any implementable measures/ steps taken by concern authorities to further strengthen and preserve the safety and security of telecommunication infrastructure and the digital eco-system as a whole.

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

TTL Response:

There are numerous Devices, Apps and websites available at various platforms which are very popular among users. These devices, apps and websites collect user's information after seeking their consent. Users may not be aware of the use of collected information by these data collectors. Users also tend to share their personal details like photographs, videos,

location, religious and political views on these web-sites and apps. The data collected by these web-sites and apps are processed and also shared by the data collectors to third party for various marketing and commercial purposes. Hence the National Privacy Principles should apply to all organisations processing personal data. It may be therefore be necessary to impose a duty on all providers of communication or equivalent services to keep the collected content in the form user information, confidential. The customer should be given a confidence that their personal data is being properly protected, irrespective of service or device.

It is therefore suggested that the authority may ensure a legislation which is service and technology neutral so that it's rules are applied consistently to all entities that collect, process and store personal data. The legislation should ensure that only relevant information, necessary for collection purpose, should be extracted from the user. Also a mechanism may be brought in place, which could continuously engage with user awareness with regards to the effect of sharing, the personal information and views in long term. Considering that a majority of the these apps and websites are hosted on servers outside the country and internet being an open access, it is vital that the user is aware of the threats and consequences of the information being collected by the data collectors and also the information being shared by the user in public domain on Social Networking Platforms.

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

TTL Response:

Yes! TTL agrees that there is a need to bring parity in the data protection norms to TSPs and other communication providers offering comparable services by applying the same set of guidelines on other communication providers and data collectors in all sectors as applicable on TSPs. The rules to ensure confidentiality of electronic communication, irrespective of the technology used, such as internet based voice and messaging service or TSPs should be common.

The issue of risk to data security and privacy cannot be addressed unless a mechanism is devised to have adequate safeguards in place, from devices and apps acting as data controllers. It needs to be ensured that the privacy needs to be guaranteed for both the content of the communication as well as the metadata. The content of communication or metadata either should be anonymised or deleted, in absence of consent from the user.

Question 11: What should be the legitimate exceptions to the data protection requirements imposed on TSPs and other providers in the digital ecosystem and how

should these be designed? In particular, what are the checks and balances that need to be considered in the context of lawful surveillance and law enforcement requirements?

TTL Response:

TTL believes that a legal framework has already been defined, which specifies the lawful surveillance rules, available to the Law Enforcement agencies in India; hence there is no requirement of introducing additional checks for the purpose of lawful surveillance at this point of time. However, we recommend a more balanced approach through introduction of a legal process, which facilitates the TSPs to challenge an LEA request, which is found to be outside the scope of relevant laws.

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

TTL Response:

No Comments