1178/TRAI/ISPAI/17

November 06, 2017

Shri Arvind Kumar,
Advisor (Broadband & Policy Analysis)
Telecom Regulatory Authority of India
Mahanagar Doorsanchar Bhawan,
Old-Minto Road, Near Zakir Husain College,
New Delhi – 110002

Subject: ISPAI Response to TRAI Consultation Paper on Privacy, Security & ownership of the data in the telecom sector

Dear Sir,

We congratulate the Authority to have come out with the consultation paper on the matter captioned above and sincere thanks for proving us the opportunity to submit our response on this matter.

We have enclosed our comprehensive response for your consideration. We believe that the Authority would consider our response in positive perspective and incorporate our concerns on the subject matter.

Looking forward for your favourable consideration.

Thanking you,

With Best Regards,
For Internet Service Providers Association of India

Rajesh Chharia
President
+91-9811038188
rc@cjnet4u.com

Encl: As above

ISPAI Response to TRAI's Consultation Paper on 'Privacy, Security and Ownership of the Data in the Telecom Sector'

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?

Response:

The privacy and data protection provisions presented in the telecom license agreement of TSPs are robust in nature with severe financial penalties for any non-compliance. However the same provisions are not being made applicable to all the entities offering similar services in Internet Ecosystem, thereby putting the consumer at risk. The consumer data handled by such entities are being stored and processed in servers located outside the country there by creating difficulties in monitoring by the agencies.

Hence the principle based horizontal rules on privacy and security of customer data should be holistically implemented on all the entities operating in Internet Eco-system irrespective of the technology used and type of services being provided.

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?

Response:

Ministry of Communications and Information Technology (MoCIT)[1] defines ***"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.*

The above stated definition is being adequate and no modifications are required. The authority should make note of difference between the personal information, non-personal or anonymous information and aggregate information. The explicit consent of the customer should be made mandatory for the personal information whereas it would not be required in case of non-personal and aggregate information during the period customer makes use of services being provided by the entity.

[1] http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf

This distinction will help in development of innovative services & help the organization to make use of big-data analytics. The pseudonymisation of personal data can provide better way to protect the data while usage without the need for explicit consent of the customer. The entities should be made liable for any negligence with privacy and protection of personal data according to the rules of the country in which the services are being offered. The entities should also adhere to the customer's right to be forgotten (when they stop the services) and help the customer to gain access to sharing his personal data by providing a technology based solution to manage their "opt-in" or "opt-out" consents. Once the customer terminates the use of service, the entities should not be allowed to store the customer data (personal or otherwise) other than which is required by the law.

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.

Response:

The rights and responsibilities of data controller during the usage of customer personal data should be similar to what the other entities have in Internet Ecosystem. The data controller should adhere to all the laws/ guidelines/ compliance requirements on privacy and personal data protection which the entities are subjected to. Customer rights and personal data protection should be respected and hence the data controller should not be allowed to have any rights which supersede the rights of an individuals over their personal data usage. The Data Controllers should be restricted from any 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?

Response:

Government has an important role in helping the industry by building the confidence of customer on the usage of his personal data by the entities. The personal data should be mandated to be kept in encrypted format and the entities should follow best practices and should disclose any breach for ensuring appropriate and immediate measures to be taken by both customers and authorities. Several access controls may be placed to ensure that the encrypted customer personal data is not being made available easily and the third parties handling personal data on behalf of entities should be subjected to the same

guidelines. The human intervention with support of technology based audit architecture (for checking and keeping track of the consent logs) will help in compliance monitoring and assessment by the entities. The compliance can be self-assessed by these entities or by accredited standard bodies like ISO for security; or by auditing firms that have the requisite expertise and capability. If necessary, the authority 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?

Response:

The new data based businesses will require the support from the authority and government in mitigating the risks and building the customer trust which help them in allowing the entities to use their personal data without any roadblocks. These businesses will help in developing innovative product offerings and lead to economic and social welfare.

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?

Response:

There should not be any government or its authorized authority to set up a data sandbox and allow regulated companies to create anonymous data sets. This may limit and create roadblock to emerging dynamic business models. The sharing of anonymized data should be left to the entities who shall share by entering into agreements as per their requirements and needs of customer.

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?

Response:

To preserve the safety and security of telecommunication infrastructure and digital ecosystem, the authority may palace some rules restricting the entities to send certain category of data (biometric and data related to critical infrastructure) outside the country. The entities should work with National Computer Emergency Response Teams when there is critical leakages or misuse of personal data which will help in minimizing the impact on consumer and the entitiry. The security norms being mandated for securing Ttelecommunication infrastructure should be extended to cover digital infrastructure of the entities 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?

Response:

The same type of communication services are being provided by several entities in the internet ecosystem. Hence the linkage of type of service to an entity is getting blurred and the internet ecosystem is presently not limited to the TSPs alone. Customer expects his/ her data to be protected in the best possible way irrespective of who is the entity is. Hence as stated earlier, the rules pertaining to privacy and data protection of personal data should be equally applicable to all the entities operating in Internet ecosystem irrespective of the technology they use and nature of services they provide. All the entities mentioned in this question should be subjected to the same rules and horizontal principles should be uniformly applied which will ensure customer protection all the time.

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?

Response:

The customer is making use of similar communication services which are being provided by several entities (Licensed or non-licensed). Other communication service provides (such as OTT) offers similar services which are equivalent to telecommunication services which are to be provided only with a relevant license authorization. Hence the principle of 'Same Service, Same Rule' should be made applicable to all these entities to effectively deal with the privacy and data protection issues.

Hence we recommend the rules should be uniformly applicable to all the entities (who operate in Internet ecosystem and such rules should be aligned with international best practices.

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?

Response:

The authority must treat all the entities equally when it come to the compliance for the rules laid out for privacy and data protection of consumer personal data. This is only possible by the way of implementing "same service, same rules". There should not be any exception for any entities who handle and process customer data where the authority should effectively be able to conduct the lawful interception of data.

These security guidelines should include other players and not just limit to TSPs alone due to the difficulties which are laid out due to strong encryption, spoofing of calling line identification and servers being located outside the geographical boundaries of the nation. We believe that rules of national security should be applied to all the entities uniformly.

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?

Response:

Presently the international trade and new business models make extensive use of cross border flow of information, which creates jurisdictional challenges to the authorities while monitoring for national security requirements. All the entities who provide the services in a nation, should be made accountable for compliance to security requirements applicable under the laws of that nation. The authority may critically examine in restricting certain type of data (financial transactions and critical infrastructure related) to be within India. These security and data protection rules should be equally applicable irrespective of technology and platform used for providing the services. Bilateral agreements between the global associations and the government would play and important role in addressing and overcoming these potential issues involved in cross-border flow of information.