Before the

TELECOM REGULATORY AUTHORITY OF INDIA

zeotap India Pvt. Ltd.
974, 4th Cross, 80 Feet Main Rd
Koramangala 4th Block,
Karnataka 560034
Bangalore, India

Phone: +91 9900000516
Email: privacy@zeotap.com

zeotap India Pvt. Ltd. and zeotap GmbH ("zeotap") submit counter comments on the consultation paper on Privacy, Security and Ownership of the Data in the Telecom Sector of August 9th, 2017.

At the outset zeotap is thankful to TRAI for giving an opportunity to offer forward-looking, practical and constructive counter comments on this important consultation paper on Privacy, Security and Ownership of the Data in the Telecom Sector. We are of the firm view that there should be uniform personal data security norms for all types of service providers to the telecom ecosystem, and no one must be allowed to collect more than needed information for providing services. Such data must be used only to provide services to the customer using telecom networks, strictly as per the law of the land and not for retaining the profile/ or for using it for other purposes.

Telecom operators do collect some personal data for customer acquisition, customer care and also generate some data during the call processing etc. Such collected personal data by the telecom operators must be allowed to be used only for providing new innovative services or generating new revenue streams in such a way that the personal sensitive information can't be used by the third party for identification of any subscriber. For this, before using or sharing such sensitive information to the third party the personal data must be de-identified and randomised at the operator's premises to the extent that any individual cannot be identified by the third party.

Looking at the comments, we find that almost all the stake holders do agree with our observations on de-identification and randomisation of personal and sensitive data.

Further, from the comments of the stake holders, it is observed that:

1. In general there is wide acceptability to de-identify the subscriber's personal and sensitive data in such a manner that the subscriber's

identity and vital attributes cannot be obtained outside the telecom operator's original database.

2. Stakeholders do agree with the provision of EU's General Data Protection Regulation ("GDPR") that anonymized data set, after stripping vital personal attributes, falls outside the ambit of rules applicable on the personal and sensitive dataset.
3. Telecom operators must be allowed to use de-identified data for commercial applications in such a manner that the identity of the individual subscribers cannot be established outside the secured telecom network of the operator.
4. Level playing field and uniform personal data security norms must be applicable to both licenced and unlicensed telecom service providers.
5. No service provider must be allowed to collect more personal and sensitive information than required for provisioning of the requisite service. For achieving this objective, we suggest service providers, such as OTT service providers, can access (i) only the requisite attributes of the subscribers; (ii) in de-identified format (so that the subscriber cannot be identified by a third party); and (iii) through an advanced and approved platform only.
6. Data controller should remain primarily responsible for meeting privacy obligations and for providing redress to individuals. So long as a data processor merely processes data on behalf of a data controller its responsibility is to follow its data controller's instructions and to assist the data controller in meeting its privacy and security obligations.
7. There is a need to look at best international practices in the interest of the subscribers and the country. In this regard the GDPR may be used as a reference point.
8. In fast changing technological environment, Government-supported sandbox approach will not yield the requisite results and may work as impediment in the process of innovation. Hence the best approach would be to have well-defined uniform rules, regulations, third party audit, quick enforcement mechanism, subscriber education and a stringent penal system.
9. In view of new emerging applications such as smart city, all sensor networks etc, it will be very difficult to get the consent of the subscriber for each application. Therefore, in the interest of the society (such as public safety), an opt-out option and use of de-identified personal data by government notification should be used.
10. There is an urgent need to work on mitigation on vulnerabilities due to NFV, cloudification, hosting of personal and sensitive data outside the sovereign control of the country, network disaster recovery and maintenance control centres outside of India, deep packet inspection capabilities of SOCs (system on chip) of the imported telecom gear equipments to name a few.