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 (collectively, "zeotap") submit these 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 applauds TRAI for bringing a consultation paper on this important subject.

This will help all the stakeholders to understand and adhere to private data security norms in this digital age. This will also give an opportunity to the policy makers to take implementable, low cost uniform regulatory measures to allow the industry to innovate new services while protecting the confidentiality of personal data of the subscribers strictly as per the recent judgement of Hon'ble Supreme Court of India. zeotap is the first global data platform successful at winning telecom operator data across three continents based on best-in-class data privacy and security. zeotap was founded in Berlin in 2014 and has further offices in Bangalore, New York, Madrid, Milan and London. The company refines and segments the data to make it safely accessible for more relevant digital advertising. zeotap is at the forefront of de-identification technology offering a solution built with privacy by design in mind. zeotap's robust privacy architecture enables us to unlock the value of device user data with minimal risk to consumers and always subject to opt-out controls. Operating in the global business environment, we work to ensure compliance with the strictest privacy frameworks around the globe including the European General Data Protection Regulation ("GDPR"). zeotap pursues the distributed data storage model where data is stored within the region of its origin, but is managed under a uniform approach featuring the state-of-the-art technology, legal and organizational safeguards. As an innovator company, zeotap sees its mission in bringing innovation that can benefit both companies and the general public.

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 to the customer. 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 (other than when the customer is willing to give consent for marketing or similar 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 cannot be used by a third party

for identification of any subscriber. For this, prior to using or sharing such sensitive information with the third party the personal data must be anonymized and randomised at the operator's premises, to the extent that no individual can be identified in any manner by the third party.

Following are our response to the questions raised in consultation paper:

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?

Answer:

In the present scenario, different data protection requirements are applicable for different players in the ecosystem. For example, telecom service providers are subjected to toughest data protection requirements, whereas OTT players, device manufacturers, OS and application software providers do collect a lot of personal data of the subscribers by taking advantage of their ignorance.

The data security conditions for non-licenced telecom service providers should not be less stringent than for telecom operators, as the former collect a lot of additional and un-necessary subscribers' personal data, more than required to provide a service. Most of such players, being foreign entities, keep such data beyond the sovereign control of the India, spill such personal data across many networks abroad, and are not obliged to follow the law of the land.

No service provider must be allowed to collect, analyse and profile more than requisite personal data for the provisioning of a particular service to subscriber unless the subscriber gives informed consent for his data to be used for marketing or similar services. The rules pertaining to the handling of subscriber data must be transparent and easily accessible to subscribers.

Telecom operators do collect and generate some personal data of a subscriber (under contract for provisioning of telecommunications service, under licence of Government of India) for customer acquisition, customer care and for call processing etc. Such personal data must be allowed to be used for providing new innovative services or generating new revenue streams. Prior to using or sharing such sensitive information with a third party the personal data must be anonymized and randomised at the operator's premises, to the extent that no individual can be identified in any manner by the third party.

A level playing field must be created for telecom operators and other service providers. The regulator/legislator should take into account the sensitivity of data and risks to the individual rather than the industry sector of the data controller. A uniform privacy regime will benefit all the stakeholders including the businesses and the general public. First, uniform rules are easier for the individuals to understand. The general public should not be expected to be educated about the differences in the legal rules applicable to their mobile usage data as opposed to the rules applicable when they stream a video on a website. Second, uniform rules promote innovation by fostering competition among service providers.

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?

Answer:

Current definition from the Information Technology Rules is similar to the one adopted in Europe (GDPR), and should be maintained as an umbrella term.

Present day technology permits to strip off vital identifiable personal information, followed by process of Anonymization and Pseudonymization of such data, at the data controllers premises, before allowing it to be accessed for any new service. Such near real time anonymized data that cannot be used to identify and locate/profile/track any individual must be kept outside of the ambit of personal data definition.

To explain further, exceptions could be carved out for identifiers that identify a device, not individual and are non-persistent, examples being cookie or Ad ID (resettable, or can be purged from the equipment).

In any case, different kinds of data that can be potentially personal should be treated differently depending on the risk that certain data poses to privacy. Data that does not include the contents of a communication, as well as individual's identity, should be treated as non-sensitive, requiring only implied (tacit) consent.

Such Anonymized and Pseudonymized data does not infringe on the right of privacy of any subscriber and hence may be allowed to be used for provisioning of new innovative services. The subscriber should be informed about available opt-out option to enable him/her to opt out at any moment of time.

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.

Answer:

Data controllers must be made responsible for transparency (notice), data security, secure processing of data and should be held responsible for any type of data breaches due to processes adopted or otherwise.

Rights of any individual are always prime and cannot be superseded by any entity. This is in line with recent judgement of Hon'ble Supreme Court regarding personal data privacy.

There must be a provision for approval and regular third party audit of the processes and personal data security systems. Such audit reports must be submitted to the concerned authorities as a condition of licence or to a designate body responsible for data protection and cyber security for the telecom sector/ country.

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?

Answer:

As suggested above in the answer to Q3, there is a need for a designate body responsible for data protection and cyber security for the telecom sector/country. This body must define and enhance Codes of Conduct for personal data security from time to time to keep in synchronization with technology and threat perception.

The standard processes involved in the data security must be defined and regularly revisited in a scientific manner to enable the innovation and new business opportunities. Regular third party audit of such processes and systems must be submitted to the concerned authorities as a condition of licence.

The technology and expertise necessary to supervise the compliance already exist.

It is necessary to make sure that such mechanisms should not at all become a mechanism for creating more red-tape and hindrance for innovation and business.

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?

Answer:

Yes, there must be dynamic and scientific measures to protect personal data, foster innovation and eliminate red tape mechanism.

It is necessary to identify data uses that pose minimal risks and also ensure that the personal data security rules are not overly burdensome (for example, with such data uses it is better to give an opt-out option instead of opt-in consent).

The designated body/ regulatory bodies must also be made responsible for solving the problems well in time (say 30 days), removing causes of delay/hindrance etc., in the process of innovation and deployment of new services. Mistakes in the processes should be condoned, but not the deliberate delays/ inaction/ wrong actions in the name of processes etc.

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?

Answer:

It should not be an authority setting up such a “sandbox.” First, aggregating all data within one data centre poses additional risks for such sensitive personal data. Second, government has, unlike the companies, no incentives to invest into the cutting edge technology.

Companies should be mandated to use state of the art technologies and processes as per direction of designated data protection agency, get regular technology up-gradation, submission of periodic third party audit and Certifications such as 27001 (or equivalent) must be considered.

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 allows the regulations to keep pace with a changing technology ecosystem?

Answer:

There is a need for a designate body responsible for data protection and cyber security for the telecom sector/ country. This body must define and enhance Codes of Conduct for personal data security from time to time to keep in synchronization with technology and threat perception.

This authorized agency must make rules and regulations for data security processes & systems in a scientific manner (to enable the innovation and new businesses). The data security processes & systems of all type of telecom service providers must go through regular third party audit. Such audit reports must be submitted to the concerned authorities as a condition of licence.

Such authorized agency must periodically/ regularly take services of reputed and independent private sector IT, Telecom and data security technical experts to review the new technical developments and data security risk mitigation strategies by looking at the best global practices. The recommendations of such experts must be made public and implemented.

Telecom is a highly regulated sector, hence it is necessary to make sure that such mechanisms should not at all become burdensome, create more red tapism and hindrance for innovation and business.

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?

Answer:

- Programmes for awareness / training of all stake holders (particularly Telecom operators and other service providers) about the personal data security threats and measures to prevent it.

- Intensive, subscriber education about the personal data security threats and their rights including through SMS and simple voice notifications concerning privacy and the data sharing policy.

- None of the technology provider (system OS, handset manufacturer, system/application/ security software download providers etc.), OTT service providers, ICT service providers (telecom, broadband, ISP, broadcaster/ multicasters etc.) must be allowed to gather any personal information that is not absolutely necessary for provisioning of the said services (unless the subscriber has given informed consent). Such information must be used in a dynamic manner only and should not be retained for future reference. In case limited profiling is needed as a part of that particular service, data access must be given in a restricted manner, after proper authorization and maintaining the log.

- Customer care facilities should work as a nodal point for customer care for all the services offered using TSP (and licenced operators) network on cost plus basis. TRAI may define such cost.

- Major OTT and other service providers having turnover/ business equivalent to (say 5 cores) must have presence in India and must come under the jurisdiction of Indian laws (and taxation).

- The subscriber must be told in very simple and clear terms, why and what personal information is being sought and what may be the implications of sharing such personal information.

- Opt out option with mandatory clearing of all historical personal data must be available to the subscribers at any point of time.

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?

Answer:

As answered in Q8.

Further, Device manufacturers, operating systems, security system and other value add service providers must be asked to implement "privacy by design." They must be held responsible for any data breach due to their systems, software or otherwise.

Recently, the MeitY has initiated actions to make sure that handset manufacturers do follow data security by design itself. This is a welcome step.

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?

Answer:

Yes, there is an urgent need to have parity on personal data collection for different communication service providers (TSPs are highly regulated infrastructure based organizations, whereas other service providers have almost free hand). However, consideration must be given to how intrusive data collection practices are and the nature of data (its sensitivities). Businesses that do not have access to sensitive personal information should have a more lenient treatment.

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?

Answer:

De-identified data that reasonably does not allow identifying the individual should not be subject to

restrictions. Also, the legitimate interests of data controllers should be taken into consideration. An open list of such legitimate interests including research, performance of a contract, and marketing (apart from unsolicited phone calls, messages and emails) could be adopted.

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?

Answer:

There should be an option for private parties to overcome the international data transfer restrictions by putting in place certain contractual and technological safeguards (standard clauses, binding corporate rules). As India is not considered by default a "safe country" by the European Union, the government should seek an international agreement on a mechanism similar to the Privacy Shield that would enable Indian companies to have access to EU data, as many Indian companies have the expertise and know how that are of interest for EU companies utilizing user data in their business. Furthermore, it will also facilitate EU companies to take help of Indian companies in analysing and processing their data.

As for as the jurisdictional criteria, the main factors should be where the data collection occurs, and whether the services in connection with which the data is collected are offered in a particular territory. These criteria would create enough predictability and certainty for the data subject without putting extra burden on companies.

The foreign entities having access to Indian telecom users personal data must be asked to follow international data transfer restrictions by putting in place contractual and technological safeguards (standard clauses, binding corporate rules that may be similar to those defined in the GDPR) and give undertaking that such data will only be used for providing agreed near real time telecom services and will not be used for any other purpose (such as profiling and/ or any other commercial, criminal or political use).

* * *

Conclusion

zeotap is not a data owner but an analytics company that uses technology to utilize data and build innovative use cases for new technologies such as Internet of Things (IoT). The need to safeguard privacy should not be a threat to innovation but rather a chance to reconcile the interests of companies and consumers. Technology is one of the keys to successfully addressing the existing threats to privacy. The task of the legislator and the regulatory authority is to provide a level playing field for different companies, enable the development of privacy protective technologies posing little risk to consumers, put reasonable control mechanisms in place, and ensure that customers have access to an adequate redress system in case their rights have been violated.

We believe the decisions by TRAI should consider the aspects discussed above in our comments and ensure that innovation does not get hampered.