



To,

The Advisor (BB & PA),
Telecom Regulatory Authority of India,
Mahanagar Doorsanchar Bhawan,
Jawahar Lal Nehru Marg,
(Old Minto Road), New Delhi-02

No: Regln/1-35/2015/

5097

Dated: 18th Oct, 2017

Sir,

{Kind Attn: Shri. Arvind Kumar}

Sub: - Comments on Consultation paper on "Privacy, Security and Ownership of the Data in the Telecom Sector".

Kindly refer to your office press release dated 09-08-2017 vide which a Consultation paper on "Privacy, Security and Ownership of the Data in the Telecom Sector" was released and sought inputs/ comments from the stakeholders. In this context, kindly find herewith the BSNL comments on the above mentioned consultation paper:

Q.1 Are the data protection requirements currently applicable to all the players in the ecosystem 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?

BSNL Reply: Data protection requirements to be fine-tuned upon vide consultation. Sharing of personal data should be with the user consent. And public awareness should be created regarding the same.

TRAI is also required to ensure that all processing of personal data is compliant with the provisions of the law of the land, and the data controllers to be able to provide evidence of compliance. A further purpose of the audit process may be used to verify that the processing complies with each of the Principles of Data Protection and to provide such evidence.

BSNL Subscriber personal data (Data given in the Customer Application form) is maintained by concerned ITPC circles. This data is used only for billing and for resolving of faults, and providing information to Law Enforcement Agencies when requested. Browsing history/ Browsing Logs are not captured nor stored in our server for any Landline Broad Band customer of BSNL.

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?

BSNL Reply: Personal Data can be defined under the following types.

Personal details: Included in this category are classes of data which identify the data subject and their personal characteristics. Examples are names, addresses, contact details, age, sex, date of birth, physical descriptions, identifiers issued by public bodies, eg Aadhar number.

Family, lifestyle and social circumstances: Included in this category are any matters relating to the family of the data subject and the data subject's lifestyle and social circumstances. Examples are details about current marriage and partnerships and marital history, details of family and other

संलग्नक (बी.पी. एफ. पी.ए.)
द्वारा सं. 1246
दिनांक 23/10

household members, habits, housing, travel details, leisure activities, membership of charitable or voluntary organisations.

Education and training details: Included in this category are any matters which relate to the education and any professional training of the data subject. Examples are academic records, qualifications, skills, training records, professional expertise, student and pupil records.

Employment details: Included in this category are any matters relating to the employment of the data subject. Examples are employment and career history, recruitment and termination details, attendance record, health and safety records, performance appraisals, training records, security records.

Financial details: Included in this category are any matters relating to the financial affairs of the data subject. Examples are income, salary, assets and investments, payments, creditworthiness, loans, benefits, grants, insurance details, pension information.

Goods or services provided: Included in this category are classes of data relating to goods and services which have been provided. Examples are details of the goods or services supplied, licences issued, agreements and contracts.)

Personal data shall be obtained only for one or limited specified purpose and for lawful purposes and is only be shared with Lawful Enforcement Agencies for security requirement, and shall not be further processed in any manner incompatible with that purpose or those purposes. It shall not be transferred to a country or territory outside the Indian Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. Further it is submitted that:

- a. ~~Subscribers should be able to see how their data are used.~~
- b. If, Data controller wants to use the data for other purposes, e.g. for marketing by the data controller's organization or passing on the data to another organization for marketing purposes, etc. the consent must be taken before sharing the same.
- c. They should be able to take it with them on leaving the service provider/ app.
- d. There should be a law which requires data controllers to use the subscriber data available with them for providing a better service only. Any commercial use of this data or handing over of the data to third party should be prohibited.
- e. Only anonymised and aggregated data (cannot be attributed back to specific individuals) may be allowed to be used by the companies who gather it to hone or develop better products and services.

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.

BSNL Reply: Data controller can use the Personal data obtained by the consent of the user, only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. Rights of Data Controller cannot supersede the Rights of an Individual over his/her Personal Data.

Notify Regulator of all processing of personal data undertaken by the Data controllers, and inform TRAI of any changes to such processing. Data Controller should Keep data safe and secure and

protects personal data against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage of personal data, Not practicing deep packet analysis. Ensure that data is adequate, relevant and not excessive. Have standards for maintenance of records with respect to processing of data, method of notification of data breach and standard operating procedure in case of such breaches, Complaint mechanisms to be in place.

The information given to the Regulator should include the purposes for which data is being processed, the data subjects about whom personal data is held, the classes of data held, recipients of that data and details of transfers of data overseas.

Q4. 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?

BSNL Reply: An audit regarding use of personal data and associated consent can play an important role in educating and assisting organizations/ Data Controllers to meet their obligations. As such, the audits across the public and private sector to assess their processing of personal information and to provide practical advice and recommendations to improve the way organizations deal with information rights issues. The authority may be given power to assess any organization's/ data controller's processing of personal data for the following of 'good practice', with the agreement of the data controller. A set of Good practices may be defined by Government/ authority for processing personal data. The focus of the audit may be to determine whether the organization / data controller has implemented policies and procedures to regulate the processing of personal data and that processing is carried out in accordance with such policies and procedures (defined by Government / organization). An audit will typically assess the organization's procedures, systems, records and activities in order to:

- a. Ensure the appropriate policies and procedures are in place;
- b. Verify that those policies and procedures are being followed;
- c. Test the adequacy controls in place;
- d. Detect breaches or potential breaches of compliance; and
- e. Recommend any indicated changes in control, policy and procedure.
- f. Identify relevant data protection risks within organizations.

The benefits of audit may include:

- a. helping to raise awareness of data protection;
- b. showing an organization's commitment to, and recognition of, the importance of data protection;
- c. independent assurance of data protection policies and practices;
- d. identification of data protection risks and practical, pragmatic, organizational specific recommendations; and

Personal information audits are being conducted in some countries. On the international front several countries have enacted data protection laws such as Canada, U.K., and Australia etc. One comprehensive piece on data protection are the EU's general data protection regulations. It regards protection of personal data therefore it should not be difficult to create a sufficiently capable workforce of auditors after due training in this field.

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?

BSNL Reply: Encouraging the content providers to host maximum contents within our geographical boundary (within the country) and with an industry friendly audit mechanism for the personal data protection.

New businesses can be created using the huge data getting generated in IT industry. However Products, services, solution, applications should be developed should include data protection & security as a core element of design & development.

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

BSNL Reply: Yes, it will be a good step in long run resulting in benefits for both the data controllers and customers.

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?

BSNL Reply: The technology solutions should be such that they provide some form of privacy (usually anonymity) for the users, such tools are being developed and are commonly known as privacy enhancing technologies. Apart from that identity-management systems may be used. Communication anonymizing tools allow users to anonymously browse the web or anonymously share content. They employ a number of cryptographic techniques and security protocols in order to ensure their goal of anonymous communication. These systems use the property that no individual can be uniquely distinguished from a group. Content may be stored in encrypted form from all users of the system. Latest Cryptography are another option.

It is important to note that technological changes influence the norms themselves. Technology thus does not only influence privacy by changing the accessibility of information, but also by changing the privacy norms themselves. For example, social networking sites invite users to share more information than they otherwise might. This "oversharing" becomes accepted practice within certain groups. With future and emerging technologies, such influences can also be expected and therefore they ought to be taken into account when trying to mitigate effects.

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?

BSNL Reply: Major Service providers of telecom infrastructures may be regularly audited for security loopholes. Proper Encouragement and support to the local Telecom manufactures for developing state of the art telecom hardware and resources. Reporting of Security related incidents to be made mandatory for the ISPs. Complaint mechanisms need to be defined wherever personal data is involved. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

Further, it is submitted that, there should be audit of the safety and security of telecom & IT infrastructures and digital ecosystem of Telecom. A knowledge sharing platform is required for:-

- a. When various breaches may be shared for taking further action to prevail future misuse of data.
- b. All TSPs & communication service provider who offer comparable services should follow same regulation for data security.
- c. Data leakage due to any reason technical or non-technical, cyber-attack so that future attacks & leakages be avoided.

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?

BSNL Reply: Most of the cases the content provider and the application service providers are taking the customer consent through an "I agree button" while doing the application installation, and using the data for analytics. This practice needs to be regulated with a proper framework.

With increasing usage of data, content, applications and advanced devices the stakeholders in these field have become an important entity who collect and have access to subscriber data.

These stakeholders however are not as legally bound as telcos are for maintaining privacy of the data pertaining to subscribers. These stakeholders, in fact, are in a more powerful position to access the subscriber data sometimes without even the knowledge of the subscriber. Therefore there should be a law in place for such stakeholders and they should be regulated in the same manner as telcos or other data controllers are being regulated.

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?

BSNL Reply: Data protection norms and practices should to be applicable to all TSPs and other communication service provider offering comparable services.

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?

BSNL Reply: The Indian Evidence Act, Indian IT Act and DOT security guidelines, define the legitimate exception to data protection requirements imposed on TSPs and other providers in the digital ecosystem. The same also defines the conditions and procedures under which lawful surveillance and Law enforcement requirements to be meet.

The legitimate exceptions may be:

- a) The disclosure is for any of the crime and taxation purposes; and
- b) is processed for the purpose of discharging statutory functions; and
- c) in case of national security purposes.


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?

BSNL Reply: Since most of the content providers are outside the country, necessary legal framework may be explored for enabling the proper use of personal data and to avoid misuses. Major content provider may be encouraged for hosting the content providers with in the country.

However, in today's world trans-border data flows a reflection of economic growth cannot be restricted/ignored in view of national data protection laws. Faced with the twin concerns about threats to personal privacy by the more intensive use of personal data and the risk to the global economy of restrictions on the flow of information, the agencies have to come up with a balanced solution.

The Hon'ble Authority is requested to kindly consider the BSNL's views/ comments on above mentioned Consultation paper.

Yours sincerely


Ved Prakash Verma
AGM (Regin-II)