

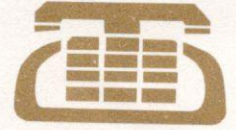
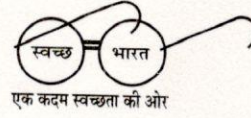
महानगर टेलीफोन निगम लि०

(भारत सरकार का उद्यम)

Mahanagar Telephone Nigam Ltd.

(A Government of India Enterprise)

CIN: L32101DL1986GOI023501



MTNL/RA/TRAI-CP-09/2017

Dated 30.10.2017

SRO (BB&PA)
[Alok Vohra]

647

To,

The Advisor (BB&PA)

TRAI, New Delhi

Sub. : TRAI Consultation dated 09.08.2017 on "Privacy, Security and ownership of Data in the Telecom Sector".

TRAI issued a consultation paper on 09.08.2017 on the aforesaid subject and asked the various stakeholders to comment on the issues involved in the consultation paper. In this reference the following comments are submitted for consideration:

Hon'ble Supreme Court recently in WP(C)- 494/2012 declared "Right to Privacy" to be a Fundamental Right imbibed under Art. 21 of Indian Constitution. The bench further acknowledged the dangers to privacy in an age of information and held that "Informational privacy is a facet of the right to privacy". During the proceedings of the matter the Union Government placed on the record an Office Memorandum dated 31st July, 2017 by which it has constituted a committee chaired by Justice B N Srikrishna, former Judge of the Hon'ble Supreme Court of India to review inter alia data protection norms in the country and to make its recommendations. The terms of reference of the Committee are :

- To study various issues relating to data protection in India;
- To make specific suggestions for consideration of the Central Government on principles to be considered for data protection in India and suggest a draft data protection bill.

The issue, therefore already being under consideration and process with Central Government for further legislative requirements, and such legislative decisions having wider jurisdiction than that of TRAI, will have implications affecting the rights & obligations of concerned parties and their civil & criminal liabilities,

पंजीकृत एवं निगम कार्यालय : महानगर दूरसंचार सदन, 5वां तल, 9 सी.जी.ओ. कॉम्प्लेक्स, लोधी रोड, नई दिल्ली-110003

फोन कार्यालय : 24319020, फैक्स: 24324243

Regd. & Corporate Office : Mahanagar Doorsanchar Sadan, 5th Floor, 9 CGO Complex, Lodhi Road, New Delhi-110 003 India

Phone Off.: 24319020, Fax : 24324243

महानगर टेलीफोन निगम लि० (जी.सी.ओ. कॉम्प्लेक्स)

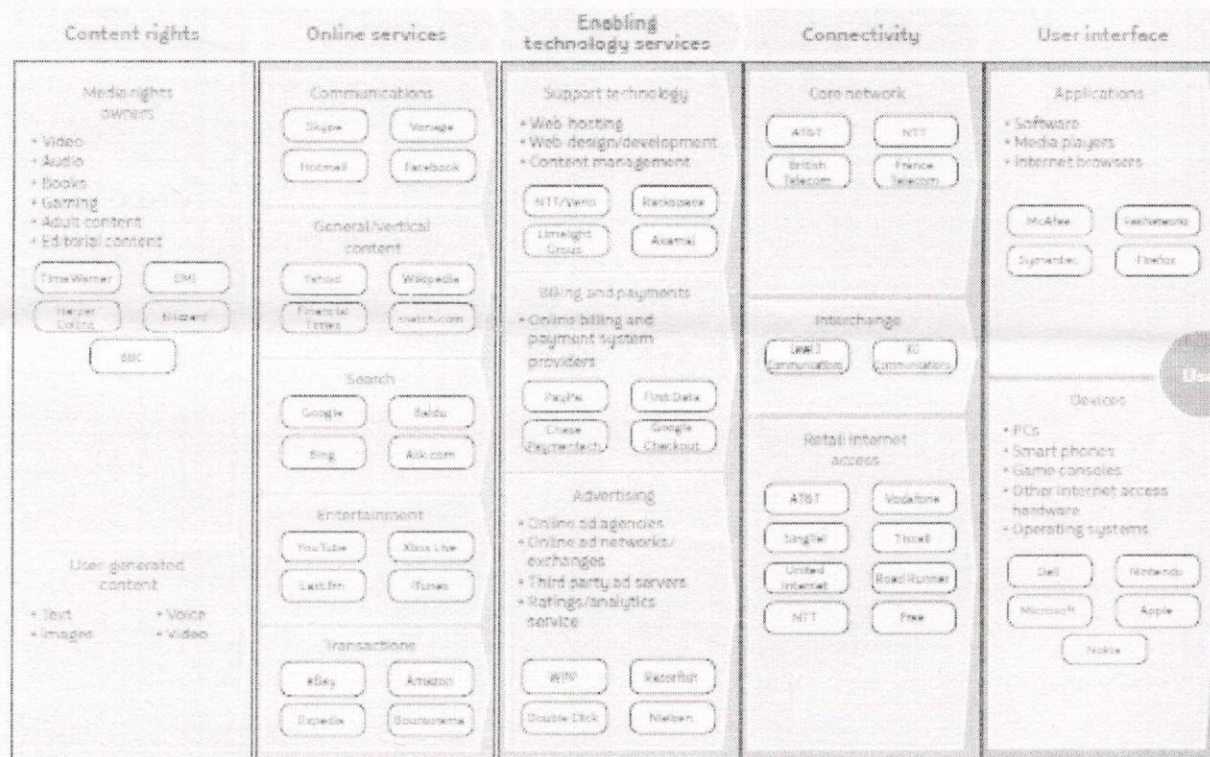
and will be applicable to all concerned domains, including but not limited to the players under the jurisdiction of TRAI.

It is therefore suggested, that for the above mentioned reasons, TRAI having only a telecom sector specific jurisdiction, may consider deferring the consultation process on the issue, till the above mentioned process of the Central Government concludes; and its outcomes and ramifications are considered, with specific reference to the telecom sector.

However, MTNL comments on the issue are submitted as below:

A. PRELIMINARY SUBMISSIONS:

As we understand, the aim of this consultation paper (CP) is to identify the key issues pertaining to data protection, in relation to the delivery of digital services; and the fundamental question which is posed by the consultation paper is the **ownership of data and who has the final right to the user's data in digital ecosystem**. Keeping this in view, MTNL's role is very specific in the digital ecosystem and this can be understood with the help of the Internet Value chain given below:



Source: AT Keany 2010

Contents Rights: Content copyright holders may range from companies whose business model is based on developing content or that hold the copyright to contents developed by third parties, to citizens who share their work and creations with others, not necessarily receiving economic compensation for doing so.

Online Services: Online service providers are companies that make different types of applications available to users, such as voice-based communication services, email, instant messaging, etc. Also included in this category are other applications that facilitate access to content, such as news and entertainment sites, search engines, commerce services, music, films or other different professional services: financial, insurance, health, etc. Players acting within these fields tend to focus their business model on advertising, although the models may also be blended, combining a free application for the user with advertising, or paying to access certain preferred services with a greater added value.

Enabling Technology Services: Companies based on technology and enabling services provide services to Internet applications such as webpage hosting, content management, invoicing and payment platforms, advertising, or providing services to third parties.

Connectivity: The connectivity link encompasses the infrastructure managers that make communications services possible, including those related to the core of Internet and traffic exchange services or retail broadband services for Internet access. **MTNL's role is limited in this arena.**

User Interface: Companies providing the interface between users and connectivity services are in charge of software applications and developing all kinds of physical interconnection devices, such as computers, smartphones, tablets and even garments and accessories for personal use, in a category recently named as the 'Internet of Things (IoT)'.

The most growing services in the Internet value chain are OTT services, many of which are broadly disseminated worldwide, with great public acceptance. They are complementary and new in comparison with the solutions already available. On the contrary, business models based on using personal data: 'If a service is for free, you are the product' give new alternative to traditional communications services, such as free applications like Skype, WhatsApp or WeChat, for example. The response of these services encourage large companies to obtain customer personal data through 'platforming' the

ecosystem by created or purchased services at each one of the links on the value chain and has given way to platforms that include the physical device, the operating system, app stores, payment methods, different communication services, storage services, development tools for third parties, and in some cases, an advertising platform. Besides, these companies the personal data are being processed and controlled by third parties also who typically do not take the consent of the user; and this is results in a one sided arrangement.

Contrary to this, TSPs also have personal information on their clients and access to their consumption parameters. Commercial exploitation of said information by Telecom Operator is relatively scarce as telecommunications companies operating under a license, concession or authorization from national authorities, unlike what tends to happen with OTT providers, are fully governed by general or sectoral rules on data protection that exist in each jurisdiction. In contracts for telephone services that operator companies in the region tend to offer, we observe that clients are assured that in accessing the service, said companies are meeting local standards, and for using data for commercial purposes or conveying data to third parties, clients normally have the option of not authorizing that their personal information be used for said purposes. This tends to be the general rule for operators.

Regulatory Framework: The most traditional part of telecommunication services is clearly defined and regulated. However, new activities in the Internet ecosystem were developed beyond regulations focused on liberalizing markets and boosting competition, such as in the former case. Regulation and the characteristics of the business being carried out at one link or another in the Internet's value chain are very different, and the regulatory framework governing these activities has not adapted to the new reality. **This creates asymmetric regulatory framework for the internet value chain. On one hand,** regulatory asymmetries between companies competing on the different markets present throughout the Internet value chain are conditioning the evolution of different players participating therein. **On the other,** they bring user rights, such as privacy, accessibility, universalness and quality of services, transparency, interoperability and portability into question.

B. POINT WISE COMMENTS:

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?

MTNL Comments: The legislation/Acts providing for Data Protection requirements are applicable to all the players in the ecosystem, and seems sufficient to protect the interests of subscribers, but its stringent implementation is required. An online dispute resolution mechanism to address such complaints exclusively, is suggested.

However the licensing/regulatory framework is applicable to only licensed service providers. Therefore, to make it more inclusive and symmetric, the data protection system should be applicable to all players in the digital ecosystem. Data protection regulations/licensing requirements should be applicable to search engines, operating systems, and online services, Mobile Apps etc, to encompass all the stakeholders in the market.

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?

MTNL Comments: In the light of advances in technology, the definition of personal data should include the information that involves the data of any third person such as Phone book contacts. User's consent should be made mandatory before sharing the personal data, of a user. Prior to taking consent, the consumer must be explained in detail about the purpose and the possible impact, of sharing of data. The following measures are suggested:

- Whenever any user's personal data is proposed to be used, a message should be sent to such user, for their denial or acceptance.
- Despite a user having given his consent, to use his/her personal data, a user should have mechanisms to ascertain who are the users of his / her personal data and should have the right to modify their use of data.
- No third party should be allowed to utilize a user's data without specific permission, from such user.

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.

MTNL Comments: The rights of the data controllers should be limited to offering services and products only. The following should be the Responsibilities of Data Controllers:

1. Obtain and process information fairly.
2. Keep it only for one or more specified, explicit, agreed and lawful purposes
3. Use and disclose it only in ways compatible with these above-mentioned purposes
4. Keep data safe and secure
5. Keep data accurate, complete and up-to-date
6. Ensure that data is adequate, relevant and not excessive
7. Retain data for no longer than is necessary for the purpose or purposes
8. Give a copy of his/her personal data to an individual, on request

In no way should the rights of a Data Controller supersede the rights of an Individual over his/her Personal Data.

For regulating and governing data controllers, an audit and certification system needs to be implemented.

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?

MTNL Comments: 100% abuse of data cannot be prevented with technology enabled architecture to Audit the use of personal Data but it will be a better mechanism. Symmetric regulation for all players of digital ecosystems may also help to reduce abuse of personal data. The development of the architecture should be done in such a manner that available manpower of skilled auditors can be used for over-riding supervision of exceptional observations collated by the automated systems.

Capable work force can be generated through training and certifications.

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?

MTNL COMMENTS: Symmetric regulations, level playing field for all players of digital ecosystems, and thorough audit controlled overall framework.

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?

MTNL COMMENTS: Yes, it will better safe-guard data, boost legitimate business opportunities without compromising on the privacy of individuals and forge a new relationship with customers, based on enhanced transparency and security that can further build trust.

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?

MTNL COMMENTS: A common data center may be set up where all the personal information has to be kept and all the internet service/ Mobile App etc will be available for download and rules should be defined clearly for downloading the service/app.

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?

MTNL COMMENTS: There already are many safety and security guidelines available for Telecom infrastructure and compliance to the same should be ensured, and the telecom infrastructure should be periodically audited and certified for availability, reliability and confidentiality.

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?

MTNL COMMENTS: As mentioned in Q2 & Q3 above for the responsibilities of data controllers, the same shall apply for every player of digital ecosystem obtaining data of individuals for any reasons.

Further, an authentic/independent rating agency/system should be evolved and Content and application service, device, operating systems and browsers

etc. may be assigned a security label/ratings based on their reliability and designs.

Though the IT Act'2000 also deals with the security of information, but further any non-explicitly consented sharing of individual information with any other agency should be made a criminal offence, equivalent to offence prescribed as "Criminal Breach of Trust" u/s 405, 406 IPC.

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?

MTNL COMMENTS: Yes, until the parity is created in application of regulatory principles among TSPs and other communication service providers offering comparable services, the concept of protection and security of individual data/information will remain a formal discussion.

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?

MTNL COMMENTS: Preliminary submissions may be referred. However, legitimate exception can be the national security, defense, maintenance of public order and interests including the prevention, investigation, detection and prosecution of criminal offences, affecting international relations of the State etc.

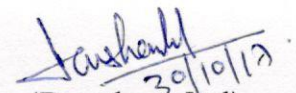
A centralized technology enabled solution which have access to the data seems to be the only solution.

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?

MTNL COMMENTS: Jurisdiction is an aspect of state sovereignty and it refers to judicial, legislative and administrative competence. Although jurisdiction is an aspect of sovereignty, it is not coextensive with it. International law circumscribes a state's right to exercise jurisdiction. The very basis of any justice delivery system, the jurisdiction, which gives powers to a particular court to accommodate a particular case, is itself being threatened over the internet.

In India, the IT Act'2000 has extra territorial jurisdiction, though for limited aspects.

Further, the principles applicable in case of cyber crimes should also be made applicable in the present context.


(Darshan Lal)
DE(RA&C)