Comments on the TRAI Consultation Paper

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?

The data protection requirements under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 are not sufficient to protect the interests of telecom subscribers.[1] The scope of the Rules extends to sensitive personal data or information which is defined in Rule 3. It includes categories such as passwords, financial information, medical information, etc. but does not include phone numbers or IP Addresses. Therefore, there is a gap in the present Rules since it is possible to share anonymized phone numbers with third parties without the consent of individual subscribers since it is not personally identifiable information, as opposed to subscriber lists which are records of IP addresses or phone numbers linked to names. The problem arises when third parties rely on such data to market to subscribers.[2] Telephone numbers and IP addresses must also be brought within the ambit of personal information. When this information is linked to other kinds of data, especially through processes like big data analytics, it is possible to identify individual subscribers.[3] Additionally, the requirement of prior consent of the data provider is often not adhered to. Thus, there is a need to impose stricter penalties for the sharing of subscriber information without consent.

With regard to ISPs, there is a need to monitor the use of cookies by websites such as Amazon which allow them to obtain IP addresses and later disclose them for targeted advertising. While an end user licence agreement or a browse-wrap agreement is a valid way to obtain user consent, data protection law can be amended to increase the standard for obtaining such consent by mandating notice individually for all kinds of information sought to be disclosed. This protects the privacy of subscribers by better informing them of the varied uses their data may be put to and then obtaining consent for the same.

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?

Several measures may be taken to incentivize the creation of new data based businesses.

---

[1] Information Technology, (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, available at http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf (last visited on November 3, 2017).

[2] https://cis-india.org/internet-governance/blog/comments-on-the-it-reasonable-security-practices-and-procedures-and-sensitive-personal-data-or-information-rules-2011 (last visited on November 3, 2017).

[3] Paul M. Schwartz and Daniel M. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 NEW YORK UNIVERSITY LAW REVIEW, 1814 (2011).

Firstly, the government can promote open data. As the data economy gains in size with businesses mining and analyzing vast amounts of data, there is a need to make this data accessible. However, India faces certain barriers to the open availability of data. One of them is the fact that vast amounts of data which companies can use are available on paper in government records, reports, etc. All this data which is potentially usable cannot be tapped into because they remain inaccessible and disorganized. Using this data can unlock unique insights into the country's demographics and society. Such data can be used by businesses to gain information about land distribution, crop coverage, age groups within a particular section of the population and thereby offer services to citizens. For instance, the US government website data.gov contains more than 85,000 data sets which can help spur innovation in this sector by increasing the amount of information in the public domain. The Open Government Data platform of the Indian government can be expanded to include diverse datasets. This includes digitizing all records and making this data freely available on a consolidated platform for businesses to use.[4] It also involves holding inter agency meetings, consultations with NGOs and corporations and public awareness campaigns to spread the message of open data to private data generators.

Secondly, the government can incentivize public corporations and government departments to transact with data oriented businesses. Government agencies, apart from being feeders of useful data can also be an important client base for upcoming data businesses. The applications of data extend to governance and the framing of new policies or legislations. Analysis of existing government data or privately mined big data from the web can help government agencies work more effectively on different issues ranging from poverty alleviation, employment schemes, maintenance of law and order, education or stimulating investment in key sectors of the economy.[5] Such insights can also help in the maintenance of public infrastructure or building new infrastructure, such as for the Smart Cities Initiative. Since the applications of this data are several, incentivizing the dealing of government agencies with data businesses is a viable strategy.

Thirdly, the government can legislate to set standards that facilitate the creation of such businesses. For instance, intellectual property rights over information of web businesses need to be such as to enable a market for such data to emerge. It must also, however, loosen IP controls for this information to be freely transferable between parties which did not create that information. Similarly, the government must enact a more comprehensive data protection bill that allows ISPs to exchange subscriber information with third party businesses which use this information for advertising. It must

[4] Joel Gurin, *The Open Data Charter: A Roadmap for Using a Global Resource*, The Huffington Post (October 27, 2015), available at https://www.huffingtonpost.com/joel-gurin/the-open-data-charter-a-r_b_8391470.html (last visited on November 3, 2017).

[5] https://www.gov.uk/government/speeches/big-data-in-government-the-challenges-and-opportunities (last visited on November 3, 2017).

also ensure that the privacy of individual subscribers is preserved when giving service providers control of this information. The government must enact changes in data protection and intellectual property law to facilitate the creation, transfer and use of such data by new businesses in a manner that preserves rights over proprietary information or of disclosure of information only by prior consent. – Aman Deep Borthakur

Question 6. Should government or its authorized authority set up a data sandbox, which allows the regulated companies to create anonymized data sets which can be used for the development if newer services?

A sandbox gives analytics professionals control of small amounts of space in data warehouses and lets them experiment with data sets in a managed environment. It decreases the amount of time that it takes a business to gain knowledge and insight from their data. It does this by providing an on-demand/always ready environment that allows analysts to quickly dive into and process large amounts of data and prototype their solutions without kicking off a big Business Intelligence project. The data sandbox can be used to find new ways in which data can be resourced, which the government can then use to create smarter policies.

Regulators try to help innovators try out their ideas, and think through the regulatory implications. Organisations like the UK's Financial Conduct Authority use sandboxes to allow new entrants to test out their products, and the potential regulatory implications, in a close dialogue with policymakers. They also commit to changing or adapting regulation in response to new entrants.[6] Acknowledging that data analytics is indispensable to the success or failure of Singapore's Smart Nation initiative, the country's government is planning to roll-out a data sandbox this year to facilitate experimentation and innovation. They are trying to align the data sets so there are more opportunities for data to be discovered and then allow interested, qualified, parties to come on board to solve new challenges.[7] Globally, sandboxes have been introduced in UK, Singapore, Australia, Malaysia and UAE. Each country has a certain target group for which sandboxing is done. All these countries have so far created sandboxed environment to support Financial Institutions (FIs) and fintech firms.[8]

The same technology can be used in the telecom sector as well as the telecom companies have little use of the data collected by them for their main business of providing service and even if they require it, they do not require identified data and can make use of de-identified data. They, however, need the

[6] https://www.fca.org.uk/news/press-releases/financial-conduct-authority-unveils-successful-sandbox-firms-second-anniversary
[7] https://e27.co/singapore-government-plans-roll-big-data-sandbox-year/
[8] http://www.thehindu.com/todays-paper/tp-business/regulators-shouldnt-restrain-innovation/article19382071.ece

consent of the customer to be able to use their data and need to put in place a system that de-indentifies such information so that it can be used for data analytics requirements.

Potential benefits of a sandbox are as follows:

- Reduced time-to-market
- Better access to finance
- Push for more innovative products
- Minimizing costs
- Regulatory Clarity
- Limited failure consequences

The government should set up a sandbox and regulate the sandbox and develop a criteria for its use that takes into account the genuineness of innovation, direct benefits to customers, risks to confidential information and the readiness of the product or service to be tested using the sand box. Adopting the Australian model of an open sandbox which is applicable to all with an option to customize for special cases seems more appropriate for the Indian Telecom Sector as compared to the system in UK and Singapore which the sandbox designed on per case basis since it will be set up by the Government and then the regulated companies can create anonymized data sets from it.

Dhanush Dinesh

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?

In the course of delivering their services, telecom and Internet service providers have the ability to gain access to a lot of information and data pertaining to their subscribers. This includes call detail records, calling patterns, location data, data usage information, etc. Though the aforementioned data is the personal data of the individual but the ownership rights, authority to use, transact and delete this data are presently ambiguous. In order to protect the privacy of users of telecom services it is important that ownership rights, authority to use, transact and delete personal data are ascertained, and to ensure that all the players in the chain are bound to follow certain safeguards while collecting, storing and using the data pertaining to their subscribers. Similarly, the role and responsibilities of data controllers should also be defined. Considering that these service providers have just as many financial incentives to sell this data and transition into a data provider for advertising and other data buyers, there is a need to ensure that the protection measures imposed on these service providers are at par with comparable services.

Providing a legal framework which provides a clear limitation of the ownership and use-rights of data generated through the use of telecom services, such as location and other meta-data is the need of the hour. This can be achieved through an over-arching privacy bill, which would ostensibly govern the use and ownership of all personal data that has been generated through the use of any commercial or government service.

Apart from legislative relief, one can require that TSPs have a set time period after which all data regarding users' meta-data is deleted from their servers in a irrecoverable form. This would ensure that users are assured that their location or call history data is not being used for whatever purposes, years and years later.

Use limitation is also necessary, to ensure that user data is not used in a manner not initially agreed upon. It becomes essential to provide caveats for usage, such that even when further use is made of the provided data (even if in a de-identified form), the data provider is in a position to provide *meaningful and informed consent* to such use. This can be ensured through

Through these reforms, it would be possible to ensure that TSPs are subject to the same standards as other messaging and VoIP services, considering the personal nature of the data generated through the use of such service is highly comparable to them. Arshita Aggarwal

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?**

Sometimes, the data stored is required by law enforcements agencies for the purposes of detection or prevention of crimes. The mechanism in such cases should be as per the mechanism provided in The Data Protection Act, 1998, which is based on the EU Data Protective Directive of 1995, is an act of the Parliament of the United Kingdom which aims to protect personal data stored on computers or in an organized paper filing system. Under the Act, the first principle of data protection is that data stored must be processed fairly and lawfully. However, there exist exceptions to the rule. When personal data is processed for crime and taxation purposes such as – the prevention or detection of crime, the capture or prosecution of offenders and the assessment or collection of tax or duty, individual rights can be restricted.[9] Only when the data is being processed for these purposes can such a request for information be entertained. Data controllers do not have to fulfill their obligations to tell individuals

[9] S.29, The Data Protection Act, 1998.

how their data is being processed or respond to a subject access request (SAR), if doing so would prejudice the crime prevention and taxation purposes.[10]

Exemptions are usually granted on a case to case basis, and the same must be done in India. The data controller making the disclosure is responsible for deciding whether or not the exemptions to the data protections requirements apply. An organization cannot apply the exemptions as a blanket policy, even if in practice there are types of information that would be made exempt in the majority of decisions.[11] *Firstly*, it must be established that not releasing the information or informing the individual about the release of the information would prejudice the investigation. *Secondly*, it must be established that there is a direct causal link between the information released and the purpose sought to be achieved. And *thirdly*, it must be shown that not granting the exemption would directly lead to prejudice. A data controller must handle each request on its own merits, and still has to provide as much personal data as possible.

The likelihood of prejudice may reduce over time, and this is particularly important to take into account when considering the application of the exemption to subject access requests. If a subject access request is made while an investigation is ongoing, there is likely to be a strong argument in favour of at least some personal data being withheld if it would reveal sensitive information about the process. However, a request which is made after an investigation has concluded is less likely to reveal information that would prejudice the purposes.

The exemption should only be applied to the extent that it is necessary to do so to avoid prejudicing the crime and taxation purposes. This means that the data controller making the disclosure must do as much as it can to comply with the usual requirements of data protection. A data controller should only disclose the information that is necessary for the purposes, and should not assume that all the data they hold is exempt. Speculative requests for personal data, especially about large numbers of people, are unlikely to meet the tests of necessity and prejudice

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?**

When requests for data are made from other jurisdictions, it becomes problematic to grant them the information as the protection that might be granted to the data by the other country may be of lower standards than the one granted by the Indian regime. Both the EU Data Protection Directive[12] and the GDPR[13] have standards for cross-border data transfers, and the same standard should be adopted in the Indian context. Cross-data transfers should only be allowed if the transfer is to be made to an adequate jurisdiction, or if the data exported has implemented a lawful data transfer mechanism. A country can

[10] Information Commissioner's Office, *Using the Crime And Taxation Exemptions, Data Protection Act, available at* https://ico.org.uk/media/for-organisations/documents/1594/section-29.pdf.
[11] R . Secretary of State for Home Department [2003] EWHC 2073 (Admin).
[12] Rec. 56-57, Art. 25, Art. 26(1)-(2), EU Data Protection Directive, 1995.
[13] Rec. 101-116, Art. 44, 45, General Data Protection Regulation, 2018.

be designated as one having adequate jurisdiction if it meets various requirements. The country must ensure an adequate level of data protection, and the adequacy shall be assessed in light of all circumstances surrounding the transfer, in particular; *firstly*, the nature of personal data, *secondly*, the purpose and duration of processing, *thirdly*, the country of origin and the country of final destination, *fourthly*, the rule of law and *fifthly*, professional rules and security measures.

A commission must be set up to evaluate cross-border data transfer requests, and such requests should only be approved if the commission deems the country adequate. Apart from the conditions already stated, the commission must take note of other factors such as the rule of law and legal protections for human rights and fundamental freedoms, existence and effective functioning of Data Protection Agreements and international commitments and other obligations in relation to the protection of personal data. If countries no longer ensure an adequate level of data protection, then their adequacy will no longer hold and the adequacy decision in their favour can be revoked.

Cross-border data transfer can take place on the basis of agreements between public authorities; however these public authorities must ensure compliance with the requirements of India's data protection regime, which should be modeled after the GDPR. Binding corporate rules will also be an appropriate mechanism for Cross-Border Data Transfers within a corporate group if they meet out the requirements set out in the GDPR. Apart from this, a Cross-Border Data Transfer may take place on the basis of an approved Code of Conduct, together with binding and enforceable commitments to provide appropriate safeguards.

- **Apurv Jain**