Unearthing the impact of the Internet on democracy in India and beyond
www.internetdemocracy.in

internet democracy project

To,

Mr. Arvind Kumar,
Advisor (BB&PA)
Telecom Regulatory Authority of India,
New Delhi

6 November 2017

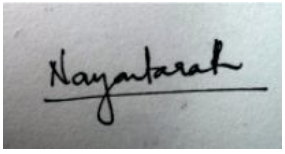
Dear Sir,

Thank you for the opportunity to comment on the consultation paper on privacy, security and data ownership in the telecom sector. Please find below the response from Internet Democracy Project (www.internetdemocracy.in) to the consultation paper.

The Internet Democracy Project is a Delhi-based civil society initiative that works for an Internet that supports freedom of expression, democracy and social justice through research, advocacy and debate in India, and beyond.

We hope that our comments will be taken into consideration.

Thank you and best regards,
For the Internet Democracy Project,



Nayantara R
Internet Democracy Project

TRAI Consultation Paper 09/2017 on Privacy, Security and Ownership of User Data in the Telecom Sector

The Internet Democracy Project (www.internetdemocracy.in) works for an Internet that supports freedom of expression, democracy and social justice through research, advocacy and debate in India and beyond.

We are grateful to TRAI for its commitment to conducting open consultations, and we welcome this proactive move to begin consultations for privacy, security and ownership of user data in the telecom sector. However, we submit that TRAI should not go as far as to recommend data protection requirements for 'all players in the ecosystem', as this goes beyond the TRAI's mandate. TRAI should stick to making recommendations for regulations to apply to telecom service providers.

In our submission, we centre users' rights over their data as part of the fundamental right to privacy[1], while balancing these with innovation in uses of data and also innovation in regulation. We recommend stepping up transparency and enabling user choice and control, along with creating data portability and redressal mechanisms in cases of compromise of user data.

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?***

Following is an overview of the data protection requirements currently applicable to protect the interest of telecom subscribers under the Information Technology Act, 2000 and its amendment, and under the Unified License:

- Section 43A of the amended Information Technology Act provides for compensation for failure to protect data. This section is applicable against body corporates at large, and not specifically against telecom service providers. It creates liability for negligence in implementing and maintaining 'reasonable security practices and procedures' by a body corporate which is possessing, dealing or handling 'any sensitive personal data or information'. The specifications of what is 'reasonable security practices and procedures' is left for agreement between the parties, or may be specified by any law in force, or may be prescribed by the central government. Similarly, 'sensitive personal data or information' is left to be specified by the central government.
- The Information Technology (Sensitive Data Protection Information) Rules, 2011, (hereafter 'SDPI rules') passed under Section 43A read with Section 87(2)(ob) of the IT Act, defines some of these terms. These rules, too, are applicable at large to body corporates, and not tailored for telecom service providers in particular. Rule 3 of SDPI rules defines 'sensitive personal data or information'. Rule 4 requires body corporates to provide privacy policies and disclosure of information, including type of information collected, the reasonable security practices, etc. Rule 5 specifies that written consent is required, and that information is collected for a lawful purpose connected with a function or activity of the body corporate, that 'reasonable' steps are taken to ensure that the person concerned has knowledge of collection and purpose. Further, rule 5 requires there be an option to opt out of providing data and withdrawing

[1] 'Informational privacy' as one of the components of the right to privacy, K. Puttaswamy v. Union of India, W.P. (Civil) 494 of 2012.

consent when data has been provided. However, the body corporate is no longer obliged to provide the goods or service for which the information was sought. Rule 7 allows for the transfer of information to any other body corporate having the same levels of data protection required under the SDPI rules. Rule 8 mentions when 'reasonable security practices and procedures' are considered to have been undertaken. It specifies industry standards that may be implemented, along with documented security control policies with managerial, technical, operational and physical security measures, 'commensurate with information assets being protected with the nature of business'.

- Section 72 of the Information Technology Act, 2000 provides for penalty for breach of confidentiality and privacy. This section creates liability for securing access to any electronic record, etc., without the consent of the person concerned and discloses the same to another person. This is applicable against any person who has secured access to data in pursuance to powers conferred under the IT Act and the rules and regulations made under it.
- Section 72A of the amended Information Technology Act provides for punishment for disclosure of information in breach of lawful contract. This section is applicable against any person, and specifically includes intermediaries.
- Clause 37 of the Unified License agreement creates an obligation upon licensees to 'ensure the protection of privacy of communication' and to 'ensure that unauthorized interception of message does not take place'.

While the above sections are useful to an extent, the nature of transactions of data is such that users are not in a position to be aware of the uses that their data is put to, the number of hands it exchanges, and what is being inferred from their data. This prevents meaningful application of the above mentioned sections.

Further, there are sections of the IT Act which create obligations for intermediaries to assist authorised agencies of the government by retaining data, as well as assist in other collection and monitoring functions:

- Section 67C of the amended Information Technology Act requires preservation and retention of information by intermediaries, for the duration and in the manner and format prescribed by the central government. 'Intermediary' is defined in Section 2(w) of the amended IT Act and specifically mentions telecom service providers, network service providers and internet service providers as included within the meaning.
- The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009, passed under powers conferred by Section 87(2)(za) read with Section 69B(3), has provisions listing the responsibilities of intermediaries, and the manner of cooperation that is required of them. These rules also prohibit monitoring and collection of traffic data or information by intermediaries without authorisation. Rule 11 requires that intermediaries maintain confidentiality in respect of directions issued for monitoring or collection of traffic data or information.

Telecom service providers are privy to all interactions of a user with the network, including the content of the interactions when the connection between the user and the servers the user is accessing is unencrypted. Given the volume and value of user data that telecom service providers are handling, a sector-specific data protection framework which accounts for the unique position of these intermediaries is needed. The risks arising from telecom service providers having access to all interactions of a user with the network are compounded by the fact that telecom service providers have to adhere to requirements to store network usage data and communications exchanged on the networks for protracted periods of time as required by government authorities. Emerging

privacy-enhancing principles like ‘data minimisation’ would be defeated where there are mass data retention requirements.

As the consultation paper rightly notes,

> Data protection in this context can be broadly understood to mean the ability of individuals to understand and control the manner in which information pertaining to them can be accessed and used by others.

A sector-specific framework is an opportunity to step up transparency, user choice and control and redressal mechanisms available to telecom subscribers. TRAI should make recommendations to the Ministry of Information and IT to have strong data protection requirements as part of license conditions.

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?

Current definitions under the IT Act and corresponding rules

Section 43A of the amended IT Act mentions ‘personal data’ and ‘sensitive personal data’. These terms are defined by the SDPI rules passed under Section 43A read with Section 87(2)(ob) of the amended IT Act.

The SDPI rules defines ‘Personal Information’ in Section 2(1)(i)

> “Personal information" means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person

The SDPI rules defines ‘Sensitive Personal Data or Information’ in Section 3

> Sensitive personal data or information of a person means such personal information which consists of information relating to;—
> (i) password;
> (ii) financial information such as Bank account or credit card or debit card or other payment instrument details;
> (iii) physical, physiological and mental health condition;
> (iv) sexual orientation;
> (v) medical records and history;
> (vi) Biometric information;
> (vii) any detail relating to the above clauses as provided to body corporate for providing service; and
> (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise
>
> Provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purpose of these rules.

This definition includes information provided voluntarily for the sake of availing the service (eg. password created, bank account details), and information that is possible to be gathered (sexual orientation). ‘Sensitive personal data or information’ is given a higher level of protection than ‘personal information’.

Below we look at the definitions that the United States, European Union and Canada use, before making recommendations about how the current definitions can be changed.

United States

User data amassed by broadband and telecommunications providers is subject to sector-specific rules in the United States.[2] Section 222 of the amended Communications Act, 1934, requires that telecommunications carriers protect the confidentiality of customer proprietary information. The Federal Communications Commission adopted a privacy framework that rests on the foundation of three principles: transparency, choice and data security, all of which are elaborated in greater detail in the order.

The order identifies three types of information collected by telecommunications service providers under customer proprietary information (customer PI). These are not mutually exclusive:
(i) individually identifiable Customer Proprietary Network Information (CPNI), defined in Section 222(h) of the Communications Act
(ii) personally identifiable information (PII)
(iii) content of communications

It adopts a 'sensitivity-based customer choice framework', which means to say that certain types of information identified as sensitive will enjoy greater protection. According to the order, sensitive PI includes financial information, health information, Social Security numbers, precise geo-location information, information pertaining to children, content of communications, web browsing history, application usage history, and the functional equivalents of web browsing history or application usage history. It also includes call detail information in voice services to be sensitive information.

Opt-in approval is required for use and sharing of sensitive customer PI, and opt-out consent is required for use and sharing of non-sensitive customer PI. There are provisions for congressionally-recognised exceptions to customer approval requirements.

European Union

The European Union General Data Protection Regulation (GDPR)[3], which replaces EU Data Protection Directive 95/46/EC, is not a telecom sector-specific regulation. However, it has useful definitions for our purpose.

The GDPR, approved by the EU Parliament in April 2016 and enforceable by May 2018, clarifies that the definition of 'Personal Information' includes IP addresses, mobile device IDs and cookie strings. This clarifies the earlier definition in the Data Protection Directive 95/46/EC, which did not explicitly name unique identifiers arising out of network interactions. Article 2(a) defined personal data as "Personal data shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". This is an important clarification, as most websites track users with unique identifiers like cookie strings and through methods like browser fingerprinting.

---

[2] https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A1_Rcd.pdf
[3] http://www.eugdpr.org/article-summaries.html

In addition to making explicit what the term 'Personal Information' includes, the GDPR introduces a new classification of data called 'pseudonymous data'. Pseudonymization is defined as "the processing of personal data such that it can no longer be attributed to a single data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." The GDPR also incentivises companies to pseudonymise data. GDPR isn't concerned with the processing of 'anonymous data', defined as " information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."

Canada

The federal Personal Information Protection and Electronic Documents Act, 2000, (PIPEDA)[4] governs data protection for private sector organisations in general, including telecommunications service providers. There are also provincial laws that govern data protection, which are similar to PIPEDA.

Section 2(1) of PIPEDA states that "personal information" means "information about an identifiable individual." Canadian courts have ruled that personal information should be given a broad and expansive definition."Sensitive Personal Data" is not defined under PIPEDA or the other privacy statutes. PIPEDA however provides that "any information can be sensitive depending on the context". This is a useful recognition, and can guide impact assessments of use of data in the Indian context as well.

According to an interpretation bulletin to PIPEDA by the Office of the Privacy Commissioner of Canada[5], personal information can include biometric information like fingerprints and voiceprints, information collected from Global Positioning System and IP addresses. Some of the principles that apply to processing of personal data of users under PIPEDA are accountability, limiting use, disclosure and retention, safeguards for personal information against loss, theft, unauthorised access, disclosure, copying, use or modification and against breaches.

Recommendations

On the basis of the definitions explored above, we recommend:

- Explicitly including unique identifiers like cookie strings, IP addresses etc. within the definition of 'sensitive personal data'. The definition should be expanded to include communications content and geolocation information also. 'Sensitive personal data' that is not essential for a service should not be collected without explicit opt-in consent. The definition of 'sensitive personal data' should be accommodative of the fact that depending on the context, innocuous fields of data can become sensitive;
- Supplement the privacy principles noted in the consultation paper with data portability and accessible redressal mechanisms. This is in addition to the principles arrived at in the Report of the Group of Experts on Privacy[6], which are noted as useful starting points in the consultation paper: notice, choice and consent,

---

[4] http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

[5] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/#fn4

[6] http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

collection limitation, purpose limitation, access and correction, disclosure of information, security, openness and accountability;
- There be a classification made in any resulting regulation, of data volunteered for the provision of the service (service tier information), and data that can be gathered. Users should be given the choice to opt out of sharing the former type of information, and opt-in to the collection and use of the latter type of information;
- Create incentives for pseudonymising data, so that the benefits that might accrue from processing user data for specific purposes may be balanced with allowing users the choice of not sharing identifiable information.

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.

The consultation paper notes the concept of a 'data controller' as introduced by the Report of the Group of Experts on Privacy.

'Data controller' is also a concept found in the EU Data Protection Directive, and subsequently also in the EU General Data Protection Regulation (Article 4(7)), understood to be the people or bodies that collect and manage personal data. Under the EU GDPR, the data controller is the authority responsible for complying with principles of data protection in Article 5(1), and the entity responsible for demonstrating consent of data subjects for the processing of their data. The data controller is also responsible for planning and implementing the policies, and ensuring adequate safeguards are in place. They are also points of contact for the national supervisory authority. The responsibilities of data controllers under the GDPR is instructive for the present consultation as well.

It should also be noted that in the context of the GDPR, merely assigning responsibilities to data controllers was found to be insufficient. In addition, GDPR introduced responsibilities and sanctions for 'data processors' as well. Data Processor is defined in Article 4(8) as "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller." Since many processing functions are outsourced to third parties, it makes sense to envision such third parties within the framework in the Indian telecom ecosystem too.

The rights of the data controller should not supercede the rights of an individual, except in cases where
(i) the data has been sufficiently anonymised, so that the data may be processed without the explicit consent of the data subjects
(ii) the data controller has to cooperate with law enforcement agencies for narrow and specific requests. The processing in such cases should be proportionate to the aim being pursued. Article 9(2) of GDPR provides for certain exceptions to processing of certain special categories of personal data, which has instructive qualifications for when the exception is in pursuance of Union or Member State law.

The EU Directive requires a national supervisor to oversee the functioning of data controllers. There is a need for an independent authority to perform this oversight function in the Indian telecom sector as well. TRAI can explore performing such a function.

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?

Technology-enabled audits are being implemented in several sectors. These auditing tools are used to track use of data in big data techniques in automated and semi-automated ways. Creating a standards-driven architecture that can support technology-enabled audits can be explored in the telecom sector as well. There have been documented risks of doing automated data processing audits.[7] These should be considered with experts, before it is concretised.

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?***

- Requirement for data controllers to collect data for explicit and specific purposes and for data processors to have a written agreement about the purpose for which they seek to use the data, to ensure that 'purpose specification' is enforceable.
- Setting up of an impact assessment body that can sign off on ethical use of data, and the implications of its use should be explored. Such assessments can be made for experiments within the data sandbox; similar to environment impact assessments, but insulated from industry capture by having transparent and inclusive composition.
- Reassessment at regular intervals to consider advances in networking technologies or business models that might have brought new threats or considerations into being.

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?***

Yes, an authority set up for the purpose may create data sandboxes which may be used for developing new services. The datasets should be tested for the ease with which the data can be de-anonymised after comparison with other available datasets. Depending on the test-runs in the sandbox, the supervisory authority and an impacts assessment body may make an impact assessment and thereafter allow or disallow those specific uses of data.

Creating and defining sandboxes can be explored as a regulatory tool to ensure that data which is consensually obtained can be put to uses whose ethical implications and regulatory compliances can be examined before it is implemented at large. This would ensure that the regulatory framework is not paternalistic towards new uses of data, but at the same time, is able to understand the ecosystem in which data is sold and processed.

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?***

'Privacy by design and privacy by default' approaches adopted by the GDPR (Article 25) are useful to think about sustainable data protection frameworks that can keep up with technological advances. Such systems also lend themselves easily to compliance monitoring. Redesigning and standardising collection and processing operations and encouraging

[7] http://www.tandfonline.com/doi/abs/10.3109/00016348209156173?journalCode=iobs20

adoption of Privacy Enhancing Technologies (PET) can help in creating a technology-enabled monitoring solution.

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?

Increased transparency and notice and consent

The lack of transparency is the first step to fix in the current telecommunications ecosystem. Users should be empowered to understand what their rights are, and given information and control over the sharing and processing of their data. Meaningful notice and consent requirements should be put in place, so that users have autonomy over their data.

The centrality of consent and the role of transparency in informational self-determination was noted in Justice Chandrachud's judgment in K. Puttaswamy v. Union of India.[8] Telecom service providers should specify on their websites and at points of sale what data they collect, how they use such data and what is the extent of user choice in these matters.

Control over personal data, including right to data portability

Users should be allowed to access data held about them, have mechanisms to correct any incorrect data, be able to revoke permission for further use of the data, and require deletion of personal data.

The consultation paper rightly notes

> In the context of data protection, it is also important to establish the ownership of the data. For instance, if the data is recognized as belonging to the user to whom it pertains, then this data becomes available for use by them to better their own lives. This brings in the dimension of empowerment to the user.

Introducing data portability would ensure that users are able to have meaningful control over their data, and are able to exercise ownership over it, as their rightful property. One of the main issues with the market for internet and telecom services, even in a relatively competitive market like the Indian one, are the switching costs involved. Introducing data portability would level up the negotiating power of users in their contractual relationships with telecom service providers, and be able to commodify their own data - something which operators and companies have been doing, but users themselves haven't had the opportunity to.

Breach notification

At the moment, there is no requirement or mechanism by which telecom service providers make data subjects aware of breaches that they might have suffered. Given the requirements under the IT Act to store user data by intermediaries, vast amounts of user data is liable to be breached. Establishing an infrastructure wherein data subjects can be identified and informed about breaches is essential for meaningful realisation of the 'right to know'.

Right to object to profiling and automated data processing

Users should be given the choice to refuse permission to profiling on the basis of their web browsing history, app usage history and any other information gathered or combined in the course of their interactions with the Internet, and still be allowed to use the service.

---

[8] Supra n 1.

Availability of redressal mechanisms

At the moment, users are not alerted when their data has been breached. Even if users should find out about a data breach because of the scale of it, the redressal mechanisms are insufficient. Even aside from the information asymmetry, the arduous process of having to file legal complaints against telecommunications companies with more resources is stacked against users. Smoothening the ability to request information held about the users by the company, and the uses to which it is being put, can strengthen redressal in cases of harms.

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?

The data protection framework for the wider ecosystem of content and service providers is not within the mandate of TRAI. Such actors will be governed by the data protection framework that would apply to any other commercial or non-commercial entity seeking to collect user data. A committee constituted for the purpose is engaged in drafting such a data protection framework.[9] While there are serious issues with the composition of the committee drafting the data protection framework, it is not within TRAI's mandate to regulate data protection for over-the-top (OTT) service providers.

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?

No, there is no need to bring about parity. Insofar as users' rights can be levelled up to ensure there is better control over their data, there can be parity. TSPs and ISPs are able to get a more comprehensive view of a user's data, so a sector-specific regulation is not out of place. Data protection by Internet-based businesses should be tackled by a different authority and not TRAI.

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?

Currently, surveillance of telecommunications data by the government is made possible in several ways:

- Section 69 of the amended IT Act gives powers to issue directions for interception and monitoring or decryption of any information through any computer resource. The section requires that intermediaries provide all technical assistance required to assist government agencies so authorised to provide access to computer resource to intercept, monitor or decrypt information.
- Section 69B of the amended IT Act provides for the monitoring and collection of traffic data through any computer resource for 'cyber security'. Intermediaries or any other persons in-charge of a computer resource are under an obligation to

[9] http://meity.gov.in/writereaddata/files/MeitY_constitution_Expert_Committee_31.07.2017.pdf

provide assistance to the authorised agency to exercise the powers under this section. Intentional contravention by intermediaries is punishable with an imprisonment which may extend to three years and is also liable for a fine.

- Section 67C of the amended IT Act requires intermediaries to preserve and retain information, for whatever duration and in whatever manner and format the central government prescribes. Here too, intentional contravention by intermediaries is punishable with an imprisonment which may extend to three years and is also liable for a fine.
- Clause 39.12 of the Unified License requires licensees to maintain suitable monitoring equipment as per requirements of the licensor or designated security agencies. conditions which impose requirements for complying with lawful interception and monitoring, as prescribed by the central government. Licensees also have to provide connectivity upto the nearest point of presence (PoP) of Multi-Packet Label Switching network of the Central Monitoring System.

The conditions under which interception and monitoring become lawful remain most opaque, when mass surveillance infrastructures like the Central Monitoring System enable the government to bypass having to request telecom service providers, thereby leaving no paper trail or accountability mechanism. Any data protection framework would also address the need for clear, proportionate and narrowly tailored requests for data sharing by governmental authorities.

A starting point for checks and balances to be instituted is some transparency and accountability around processing of personal data for law enforcement purposes. Such an accountability is in line with practices in other countries, at least on paper. The EU Directive 2016/680 on Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, for example, creates a degree of accountability for the data sought by law enforcement authorities.

Government and law enforcement requests or systematic arrangements of data sharing cannot be outside the purview of data protection frameworks. However, strengthening accountability on this front would require several arrangements already in place to be altered. The confidentiality requirement in the IT rules (monitoring of traffic data), the lack of information about the status and functioning of the Central Monitoring System etc. are some examples where there needs to be a drastic change for meaningful exercise of the right to privacy of Indian citizens. Checks and balances will be meaningful only if a body independent from the one involved in the said data processing functions performs them.

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?

Cross border data flows should be a concern for TRAI only insofar as foreign telecommunications firms are dealing with the data of Indian citizens. Content and service providers' handling of user data should not be dealt with by TRAI. Foreign telecom firms handling Indian citizens' data should be required to comply with the standards of the Indian data protection framework.