Counter Comments on the TRAI's Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector

Amber Sinha[1]

Centre for Internet and Society, India

November 21, 2017

[1] The author would like to thank Aditya Bhupatiraju and Viraj Gaur for their help with this submission.

1. Preliminary

This submission presents comments by the Centre for Internet and Society, India ("CIS") on the Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector published by the Telecom Regulatory Authority of India dated August 9, 2017. CIS has conducted research on the issues of privacy, data protection and data security since 2010 and is thankful for the opportunity to put forth its views. CIS made a submission was made on the Consultation Paper ("Submission") On November 6, 2017.[2]

This submission is divided into three main parts. The first part, 'Preliminary', introduces the document; the second part, 'About CIS', is an overview of the organization; and, the third part contains the 'Counter Comments' on the Consultation Paper, taking into account the submission made by other stakeholders.

2. About CIS

CIS is a non-profit organisation that undertakes interdisciplinary research on internet and digital technologies from policy and academic perspectives. The areas of focus include digital accessibility for persons with diverse abilities, access to knowledge, intellectual property rights, openness (including open data, free and open source software, open standards, open access, open educational resources, and open video), internet governance, telecommunication reform, freedom of speech and expression, intermediary liability, digital privacy, and cybersecurity.

CIS has conducted extensive research into the areas privacy, data protection, data security, and into the telecommunications sector. CIS values the fundamental principles of justice,

[2] The Submission is available at http://trai.gov.in/sites/default/files/CIS_07_11_2017.pdf.

equality, freedom and economic development. This submission is consistent with CIS' commitment to these values, the safeguarding of general public interest and the protection of individuals' right to privacy and data protection. Accordingly, the comments in this submission aim to further these principles.

3. Counter Comments

3.1 Sufficiency of existing data protection regime

Contrary to what has been argued by a few submission made to TRAI,[3] CIS believes that the existing framework does not sufficiently protect the interest of data subjects. As highlighted in Section 4.1 of our Submission, the existing framework of data protection laws in India, is inadequate to comprehensively protect the rights and interests of telecom subscribers.[4] These laws and policies do not provide adequate protection with the respect of the following matters:

3.1.1 Limited Protections for Personal Information

The data protection rules under Section 43A apply only to a narrowly defined category of 'sensitive personal data' and not all forms of personally identifiable data.

[3] http://trai.gov.in/sites/default/files/ISPAI_07_11_2017.pdf; http://trai.gov.in/sites/default/files/COAI_07_11_2017.pdf; http://trai.gov.in/sites/default/files/ACTO_07_11_2017.pdf;
[4] State of Privacy in India, Privacy International - https://www.privacyinternational.org/node/975

3.1.2 Lack of Regulation of the Public Sector

Section 43A rules apply solely to body corporate and are not extended to the public sector resulting in a lack of data protection standards for collection and use of data by public sector entities.

3.1.3 Inadequate definitions of Personal and Sensitive Personal Data

The definition of personal data is limited to data that is likely to be available with body corporate resulting in a narrow definition that excludes data that may be available with other types of entities. Such narrow definitions ignore the overlap between non-PI, PI, SPDI.

3.1.4 Inadequacy of provisions on privacy policies

Requirements of Privacy policies need to be strengthened in various respects like requiring notice prior to collection, communication through accessible and intelligible means and notification of users about any changes in the policy.

3.1.5 Inadequacy of provisions on consent

Herein, scope of consent is limited to SPDI and there is a lack of pre-defined standards for consent notices in order to make sure the consent is informed. Consent has been defined to be a one time mechanism not requiring renewal when modifications are made to the privacy policy. 43A also does not require the opt-out mechanism of consent to be easily accessible and implementable by the user.

3.1.6 Limited Access and Correction protections

Data access for users is limited to the information that they have provided, ignoring present day mechanisms that collect data both directly and indirectly. There also exists a lack of rules and standards requiring data to be made available in a structured intelligible format along with the option to edit or move the collected data.

3.1.7 Broad data retention terms

The purpose and collection limitation of 43A are applicable only to SPDI and not all personal data. Even these standards fail to connect the purpose limitation to the purposes and use consented to and tied to the duration of a service.

For a more detailed notes on the above issues, please refer to Section 4.1 of our Submission.

3.2 Questions of regulatory parity between telecom companies and OTT service providers

A few of the submissions call of greater arity between rules applicable to telecom companies and other OTT service providers. The data protection law in India should be neutral to technology and platform, and must apply equally to all data controllers including telecom companies, and OTT content and application service providers. The obligations of telecom companies are addressed in the Unified Licenses entered into the Department of Telecommunications, and there is no need to extend these contractual obligations to any other stakeholders. Instead,

the mechanism for regulating other stakeholders should be the data protection legislation. It is recommended that the Unified License is harmonized with the data protection legislation. It is further recommended that any data protection norms applicable to communication service providers such as telecom companies, and OTT service providers which provide comparable services such as messaging and VOIP services, must be privacy preserving and enhancing but not limiting in any way. Therefore, any regulations regarding communication encryption must only specify minimum thresholds, and not limit the level of privacy protection that these services may provide.

3.3 Differential treatment of different kinds of data

While personal information, including personally identifiable information and sensitive personal information is governed by data protection law, personal information in the public domain is not. A potential research question is to understand how two competing areas of policy, i.e data protection and open government data policy govern them. Personally Identifiable Information (PII) includes any information that relates to an identifiable, living person which can be used to identify that person. This includes unique identifiers, direct identifiers and indirect identifiers. Personal information where the identifiers are replaced with pseudonyms or pseudo-identifiers is a way in which data controllers try to leverage PI without the associated harms to the data subject. Anonymised information is personal information where the identifiers have been eliminated. Anonymous and pseudonymous information effectively exist in a regulatory vacuum between personal data policies and open data policies which leads to a reconsideration of the scope of data protection law. Some harms and some benefit may occur regardless of regulation, however, both regulation and deregulation are needed to solve the optimization problem of big data ie. unlocking benefits whilst mitigating harms through both substantial and procedural laws. Some regulatory

options may be developed ground up as self-regulatory or co-regulatory standards.

The process of de-identification removes identifying information from a dataset such that remaining individual data cannot be used to personally identify specific individuals, thus reducing the privacy risk of further sharing and processing of data. The different approaches to de-identification include removal of direct identifiers, pseudonymization, De-identification of Quasi-Identifiers, field based de-identification, privacy preserving data mining and publishing. Effective employment of these techniques would involve regulatory bodies to frequently examine the efficacy of these techniques in light to emerging re-identification approaches, incentivising and/or mandating the use of de-identification techniques based on the sensitivity of personal data in question through sectoral regulations.