INTERNET FREEDOM FOUNDATION

To,
Shri Arvind Kumar,
Advisor (Broadband & Policy Analysis)
Telecom Regulatory Authority of India
arvind@trai.gov.in ; bharatgupta.trai@gmail.com

November 21, 2017

Dear sir,

Re: Counter-comments by the Internet Freedom Foundation on the Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector

In furtherance to our comments to the TRAI on its consultation paper on Privacy, Security and Ownership of Data we are making counter-comments below. We restate our key asks from the present consultation seeking TRAI's endorsement of a comprehensive rights based data protection law that is enforced by a data protection authority or a privacy commissioner. In the interim, till such a law is made, various proposals made for protecting user privacy in the telecom sector may be considered including focussing on reforming the existing practices on telecom and data interception as well as surveillance.

Our counter comments seek to substantiate that any interim regulatory measures on telecom service providers by the TRAI - and the future application of horizontally applicable privacy principles by a comprehensive statute - must seek to protect people and hence their data. Our policy focus in India must not be focused on how to facilitate the economic exploitation of our citizens data. It is important to consider this in a human rights framework rather than with a limited analysis of privacy being a property right limited to mere "ownership". As advanced in our submissions, this is a consistent reading with the *Justice Puttaswamy* 9 bench judgement of the Supreme Court.

Below, we specifically indicate substantive concerns as well as endorsements of points made in the comments of Airtel, Baijayant "Jay" Panda, Business Software Alliance (BSA), Cellular Operators Association of India (COAI), GSM Association, Takshashila Institution, Isprit and the Internet and Mobile Association of India (IAMAI).

1. **Airtel**

    a. We dispute the submission made by Airtel that provisions for data protection in the telecom license agreement are adequate. Specific reference is made to our submissions whereby we indicated that the present provisions of the

license prevent the deployment of bulk encryption across networks, probable ad and tracking injection by telecom service providers and further the problematic surveillance regime applicable for interception. Further, somewhat anecdotally any telecom user in India is aware through personal experience of an absolute failure by service providers and regulation to protect their identities from marketers and spammers many of whom claim to be agents of telecom companies.

b. The claims for parity in regulation, and vertical application of data protection principles is to be commended as a task which may fall for consideration of a Data Protection Authority however the present framing seems to incorrectly suggest, (a) the TRAI should not exercise its regulatory power over Telecom Service Providers on such issues in the interim (over whom it has jurisdiction to do so); or (b) the TRAI should exercise its regulatory power over Internet Services and Platforms if it chooses to exercise it in the telecom sector (over whom it lacks jurisdiction to do so). As stated in our submission the TRAI should urgently look to advance privacy and data protection in the telecom sector by focussing on Telecom Service Providers.

c. Further we are concerned with the repeated appeal for a carve-out for large data sets from any possible privacy or data protection regulation. “Big data” by itself relies on the use of granular bytes of individual data which are personally identifiable. Even after anonymisation, such data can be analysed and processed to again become identifiable. In terms of principles, privileging the interests of economic exploitation of data over the rights of individuals to it’s protection will be inconsistent with the objectives of the present consultation and also the nine judge bench decision of Justice Puttaswamy which held in favour of the fundamental right to privacy.

2. Baijayant “Jay” Panda

a. We endorse the comment by Shri Baijayant Panda where he has stated that personal data generated through machine learning algorithms should be included in the definition of personal data. We also commend the Hon’ble Member of Parliament for his endorsement of the principle of consent, and hope his support for it is to it’s fullest extent including consent being a necessary pre-condition for any state based scheme or program.

3. BSA

a. While some parts of the submission may be complimentary for user rights at several instances it fails in such consistency in it's very framing by statements such as, "Most of this data being generated is not personal data." The basis of this assertion is a report made by BSA itself titled as, "What's the big deal with data" which does not disclose the methodology or any support for this assertion within it. We would dispute this assertion given that most data is user generated and can lead to identification and profiling.

b. BSA has further appended it's own data protection principles which seem to have been developed without any public interface and would tremendously undermine not only user rights but the ability of any data protection authority to implement meaningful regulation. For instance, the BSA principles advocate for a complete unhindered cross-border flow of data without adequately listing the limitations which are referred by the OECD principles it draws for support. Hence, there is an absence of comment by BSA on Principle 17 of the OECD principles that prescribe limitations on cross border flows of data unless, (a) the other country fails to observe the OECD principles; and (b) certain sensitive classes of data may be prevented for export as defined in a privacy and data protection law. We would recommend caution and scrutiny before further consideration of BSA's privacy principles framework, given its likelihood to undermine user rights.

4. COAI

a. We support COAI's submission at the Preamble (Para G), where it makes reference to the TRAI's recommendations on cloud computing. This is specifically on the following points, (a) recommendation for a comprehensive privacy law; (b) adoption of the privacy principles by the Committee of Experts under the Chairperson Justice (Retd.) A.P. Shah.

b. We are encouraged by COAI's endorsement of transparency principles and wish to state that this may not only be applied for telecommunication surveillance to Government but also to telecom companies which should issue periodic reports publicly on all interception and surveillance requests.

c. We support COAI's submission for amendment of MLAT's for the provision of requests for lawful interception given such practices are today followed informally and no clear legal authority exists for it. Further, we request that any such amendment also needs to consider the larger issue of surveillance reform as indicated by us in our submissions.

d. We strongly dispute the COAI submission on the following submissions:

   i. Adequacy of the present privacy protection for telecom users under the existing license conditions.

   ii. Sufficiency of the definition of, “personal data” and, “sensitive personal data” as defined under provisions of the IT Act.

   iii. Comments, “anonymised” and, “big data” that have previously been responded in comments pertaining to Airtel.

   iv. Though we support the horizontal application of privacy and data protection principles, we object to the slogan of, “same service, same rules” given its past use for disambiguation in the Net Neutrality consultations.

5. GSM Association

a. IFF supports GSM Association’s suggestion of a horizontal approach to the application of privacy principles by a comprehensive user rights based data protection law.

b. With respect to several comments made by GSM Association we wish to restate our submissions and specific counter comments to Airtel and COAI.

6. Takshashila Institution

a. We are largely supportive of the submission of Takshashila Institution given its framing and focus on advancing user rights within a human rights framework.

b. At the same time we are concerned with the seemingly trade-off which is created between consent and a, “accountability framework” [“consent based model is inadequate”; “consent fatigue”]. It is our belief that any accountability framework needs to be tethered to individual constituents of informational privacy which start with individual consent. We resist any calls to weaken consent as a basis for data protection in India as it would seek to cater to the needs of economic exploitation of data over user rights. For accountability to be meaningful, it has to consider the substantive basis for which it is being demanded. Here we find the proposed framework in response to Q. 3 insufficient and recommend reference not only to the

Justice A.P. Shah Report but the recently adopted EU GDPR and the *Justice Puttaswamy* judgement which articulates the principles of proportionality and necessity.

c. Further comments on audit and the proposal for, "learned intermediaries", is only one of the several measures which will ensure a meaningful implementation of any data protection and informational privacy framework. The first pillar of this will be strong, independent regulator such as a Data Protection Authority or a Privacy Commissioner which will be complemented with pro-active reporting, implementation of privacy by design and the publication of transparency reports. Compliances in terms of the scale, sector and type of enterprise will be determined within the broad privacy principles as stated in counter-comment 6(b).

7. Ispirt

a. We are deeply concerned with the framing of Ispirt's submissions which contains commentary such as, "[people may be] data rich before they are economically rich". This in its essence views users data for economic exploitation rather than protection. We strongly object to such framing as it conflicts with our submissions for a data protection framework built upon the Indian Constitution's fundamental rights.

b. We are surprised to note that Ispirt's submissions advocate for network encryption technologies subject to, "deep packet inspection" that would completely undermine any individual privacy. It is also a matter of deep regret that such, "deep packet inspection" has been suggested for use in, "network management" that would conflict with any technical protections for net neutrality.

c. We strongly object to the suggestions by Ispirt with specific reference to placing of telecom data in Digilocker and the Electronic Consent Framework. By putting such data in Digilocker by default it will by default data silos and lead to incredible privacy harm. Hence, instead of protecting user privacy or advancing any meaningful data protection such a proposal will in all likelihood cause grave damage. Further comments on the use of anonymised data, where it has been suggested by Isprit that consent may not be required is also objected given it, (a) wrongly classifies big data or anonymised data as being unable to lead to personally identifiable data on processing and analysis; (b) undermines the principle of consent required for the extraction of any granular data even to a large anonymised data set.

d. We are further concerned and object to Isprit's submissions on:

   i. It is significant that rather than listing the rights of users which is the scope of the present consultation Ispirt has chosen to instead list the rights of data controllers.
   ii. Advocated for the use of technology solutions for monitoring compliance as well the support for a government mandated data sandbox. There is little to no support for such proposals even from other stakeholder inputs given their technical infeasibility and lack of clarity as public policy proposals within the present consultation.

8. IAMAI

a. The proposals with respect to self-regulation made by IAMAI are not only contrary to the everyday harms caused by the indiscriminate collection, aggregation, analysis and disclosure of data but also in contravention of the *Justice Puttaswamy* nine judge bench judgment which has specifically noted a positive obligation on the State to make a data protection law to protect users. Hence, any self-regulatory approach, which seeks to pro-actively factor in the, "cost of compliance" would prefer the rights of business over the privacy rights of users.

b. We strongly oppose the suggestion that for a Internet of Things (IOT) model to flourish that the consent and notice model needs to be modified for simultaneous sharing of data. Such a proposal is incredibly regressive for user rights as it would allow unhindered large scale collection of data and little to no data protection for users.

c. We would restate our request for a mix of pro-active and grievance redressal mechanisms which would best ensure the implementation of privacy by design.

We hope the TRAI considers our counter comments and they add value to its recommendations.

Sincerely,

Team Internet Freedom Foundation (IFF)
@internetfreedom