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

November 06, 2017

Dear sir,

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

The Internet Freedom Foundation (IFF) is a non-profit organisation created by members of the SaveTheInternet.in movement for net neutrality. Over one million of our fellow citizens wrote to the TRAI in April 2015 as part of the consultation paper on OTT services using the SaveTheInternet.in platform, and continued to engage the TRAI and the Dept of Telecommunications on subsequent consultative exercises in this area.

IFF aims to promote the rights of Indian Internet users — freedom of speech, privacy, net neutrality and freedom to innovate - before policymakers, regulators, the courts, and the wider public sphere. We are grateful to submit our views in the consultation on consultation on Privacy, Security and Ownership of the Data in the Telecom Sector.

Our public advocacy and work on informational privacy and protecting the rights of Indian citizens vis-a-vis their data includes:

1) **Advocating for a comprehensive rights based data protection law:** Requests to pass a comprehensive data protection bill to protect privacy of users coming shortly after the historic right to privacy judgement by the Hon'ble Supreme Court of India [link]. IFF has aided Indian lawmakers in their efforts to advance proposals to create comprehensive laws to further provide for the protection of informational privacy and data.

2) **Accountability for the collection and transfer of data by private companies and large platforms:** IFF was granted permission by the Hon'ble Supreme Court to be added as an intervening party in the Whatsapp-Facebook data sharing case where we have pleaded for further disclosure of corporate data collection and transfer

practices as well as called for interim orders to protect the interests of our fellow citizens [link].

3) **Regulatory caution to protect user privacy:** Participation in past TRAI consultations where we have highlighted the urgent need to protect user privacy, including:
    a) Inputs to the WiFi Consultation highlighting various concerns [link]
    b) Response to the Free Data Consultation [link] and our concerns on the recommendations made by the TRAI [link]
    c) Response to the consultation paper on Net Neutrality [link]

As we support privacy, security and the rights of users to control their data, the present submission makes an argument for the most effective form of regulation through a comprehensive data protection law.

To broaden stakeholder comment and inform a larger number of people, we also prepared a 5 page summary of the present consultation paper to help citizens in understanding the issues at play in this subject and empower them to be better placed if they wish to provide their views to TRAI [link].

Concerns

Even though we support any regulatory measure to protect user privacy, we have some concerns with the framing of the present consultation. Our topline, concerns are as follows:

- **A comprehensive rights based data protection statute:** Data protection is about protecting the privacy of users by advancing their rights vis-a-vis their data. We have consistently advocated for a comprehensive, rights based data protection framework. A key pillar of a comprehensive, rights based data protection litigation is enforcement and accountability through an independent privacy commissioner or data protection authority. We request the TRAI to not go beyond the powers under the TRAI Act and the Telegraph Act. Any TRAI regulatory outcome from this consultation stay within its jurisdictional mandate to protect user privacy with respect to the telecom service providers in the interim till a comprehensive data protection act is passed.

- **A rule of law framework:** We are troubled by the framing of the consultation paper which seeks to advocate that a "*technology framework... will enable the regulator pro-actively monitor the system, as well as bring in advanced techniques for fraud detection*". This seems to suggest a technical framework that undermines consent,

purpose limitations and accountability (consent is one of the primary principles of data protection).

- **Big data is personal data:** The focus to fork out, "big data", from the definition of, "personal data" will undermine citizen rights. Aggregated data sets which are based on individual information have tremendous data protection implications. In all measures we recommend at the very least adoption of the Justice A.P. Shah Committee principles along with proportionality and necessity as articulated in the 9 judge bench decision in *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India* [W.P. (Civil) No. 494/2012] [link]. The principles of the 9 judge bench decision are inherent to any recommendation that may be made by a statutory authority.

Suggestions

- **Privacy and Data Protection is a rights based concept**: We urge the TRAI to agree and adopt the framing of informational privacy and data protection as not merely a property right in which, "ownership" vests with a user, but even above and beyond which in which a person has inalienable rights. These rights apply horizontally both to state and private entities and are to be enforced both by a specialised regulator such as Data Protection Authority, or a, Privacy Commissioner and through a system of adjudication in which users can make complaints. We believe TRAI must now consistently advance a position based off the foundation of privacy being a fundamental right of all Indian citizens.

- **Protect against mass surveillance:** The consultation paper at para 2.6 notes several provisions of the Indian Telegraph Act, 1885, rules and the UASL license made under it. It is relevant to note that despite such provisions only permitting individualised interception there are widespread reports of mass surveillance being carried out in the telecom sector. Reports have also indicated the use of invasive technical and commercial tracking technologies by telecom service providers in India, including the use of UIDH tracks or "super-cookies" [link]. We urge the TRAI to exercise its regulatory powers and start a public consultation and an investigation into unlawful and unconstitutional practices regarding mass surveillance and service provider collection of data on mobile, internet and landline users in India.

- **Aid and complement transparency:** The TRAI has a longstanding tradition of public consultations which are carried out in an open and deliberative manner. At present the Justice (Retd.) B.N. Srikrishna Committee of Experts established by the Union Ministry of Electronics and IT is considering the issue of a data protection framework. As noted by about 22 eminent individuals in an open letter, in addition to it's problematic composition, an issue of concern is the lack of transparency in its

proceedings [link]. Given that any recommendations or draft bill on data protection will have a wide ranging impact we urge the TRAI to share the practices adopted by it for public consultation with the Justice Srikrishna Committee of Experts.

We hope the TRAI takes forward the specific suggestions made by us against each of its queries.

Sincerely,

Team Internet Freedom Foundation (IFF)
@internetfreedom

Response by the Internet Freedom Foundation (IFF)

Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector

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?

Answer summary: *The present data protection requirements are inadequate and completely deficient to ensure any meaningful data protection or informational privacy to users, especially telecom subscribers. Given large amounts of personal data are transmitted through smartphones, in addition the existing regulations, a comprehensive legislation needs to be made following the principles of the nine-judge bench judgement on the right to privacy.*

1. The existing regulations applicable to data protection and informational privacy as culled out from various statutes and the UAS license predate the advent of smartphones and the tremendous amounts of personal data which is generated, collected and transmitted through them. This requires urgent legislative attention as recognised by the government in constituting the Justice B.N. Srikrishna Committee of Experts to recommend data protection principles and suggest a draft legislation. Even though we support this move in principle, we note its problematic composition and its lack of transparency. We urge the TRAI to share it's best practices on public consultation with the committee.

2. Any data protection regulation must necessarily follow the historic nine judge bench judgement of the Supreme Court on the right to privacy. The judgement *interalia* in its majority decision states that, "[i]n the context of Article 21 an invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair, just and reasonable. The law must also be valid with reference to the encroachment on life and personal liberty under Article 21. An invasion of life or personal liberty must meet the three-fold requirement of, (i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them.." [Chandrachud J., at Para 3(H), Part T, Pg. 264].

3. Though Chandrachud J. by himself does not comment on the, "proportionality" element it is closely linked to the requirement as applied to adjudications in the European Union. Kaul J. states the test of, "Proportionality and Legitimacy" as a heading to Para 71, in which he lists four ingredients that includes, "the extent of such interference must be proportionate to the need for such interference;".

4. We urge the TRAI to agree and adopt the framing of informational privacy and data protection as not merely a property right in which, "ownership" vests with a user, but even above and beyond which in which a person has inalienable rights. These rights apply horizontally both to state and private entities and are to be enforced both by a specialised regulator such as Data Protection Authority, or a, Privacy Commissioner and through a system of adjudication in which users can make complaints. In addition to this continuing accountability is observed with adoption of, "privacy by design" in which technology products and services conform to legal principles and standards. We are constrained to highlight that the present consultation paper was released in a contemporaneous timeline of TRAI being the only statutory body - besides the UIDAI - that argued against the fundamental right to privacy in the Supreme Court of India in the historic nine-judge right to privacy case.

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?

Answer summary: *We would caution against the recasting of the definition of personal data. Consent is the bedrock of any data protection regulation. It is pertinent to mention that consent is a continuing right which is not irrevocably assigned and a user continues to have rights over their data even after its collection. To ensure the principle of consent is meaningfully given to users, accountability systems need to be implemented by adoption of a, "privacy by design principle". This requires a mix of legal controls and technical standards that are adopted by service providers and enforced by a data protection authority.*

1. The focus to fork out, "big data", from the definition of, "personal data" will undermine citizen rights. Aggregated data sets which are based on individual information have tremendous data protection implications. In all measures we recommend at the very least adoption of the Justice A.P. Shah Committee principles along with proportionality and necessity as articulated in the 9 judge bench decision

in *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India* [W.P. (Civil) No. 494/2012] [link]. The principles of the 9 judge bench decision are inherent to any recommendation that may be made by a statutory authority.

2. The importance of, "consent" is expressly noticed by Kaul J. in his concurring opinion in the privacy judgement when he also comments on the design of any such legislation when he states, "*I agree with Dr. D.Y. Chandrachud, J., that formulation of data protections is a complex exercise which needs to be undertaken by the State after a careful balancing of privacy concerns and legitimate State interests, including public benefit from scientific and historical research based on data collected and processed. The European Union Regulation of 2016, of the European Parliament... may provide useful guidance in this regard... The state must ensure that information is not used without the consent of users and that it is used for the purpose and to the extent it was disclosed...Thus, for e.g. , if the posting on social media websites is meant only for a certain audience, which is possible as per tools available, then it cannot be said that all and sundry in public have a right to somehow access that information and make use of it.*" [Kaul J, Para 70, Pg. 36]. Hence, "consent" is an inherent facet of the fundamental right to privacy.

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.*

Answer summary: *We would restate that the focus of the present consultation should be recast towards TSPs and improving the privacy and data protections standards applicable to them in the interim till a comprehensive data protection law is made. For instance all TSPs should publish privacy policies, must be obligated to report any data breaches to affected users in addition to TRAI and the Dept. of Telecom, and penalty provisions must be used to enforce this.*

1. As stated before the jurisdictional ability of TRAI to define norms for compliance for, "data controllers" is limited. Hence, it must first examine the existing privacy and data protection provisions in the telecom sector as applicable to TSPs which need greater enforcement and improvement. This may be adopted as a stop-gap method in the interim till a comprehensive data protection framework is made through legislation.

2. It is our submission that user rights are paramount in any data protection and informational privacy legislation. Data protection is not about protecting data, but protecting the user.

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?

Answer summary: *We are troubled by the framing of the consultation paper which seeks to advocate a, "technology framework... will enable the regulator pro-actively monitor the system, as well as bring in advanced techniques for fraud detection". This seems to suggest a technical framework that undermines consent, purpose limitations and accountability (consent is one of the primary principles of data protection).*

1. The adoption of a technical framework without adequate development of a rights based data protection framework may not provide any solution for data security or individual privacy. For instance the Digilocker Framework has an inadequate understanding or protection of consent [eg. refer, "core features" which notes, "Note that issuers may directly expose documents that are public in nature (e.g., land registration or voter card) independent of the digital locker scheme"] [link].

2. We may also indicate that such a system would by itself be a form of data centralisation and pose risks to users. There are further problems in its implementation as it would in a sense be a universal backdoor to all internet applications and services. Hence, without adequate security such a compliance system by itself may pose as a security risk. There may also be onerous compliance issues, where instead of a "privacy by design" which is implemented in each online application or service by the provider through a mix of legal and technical control a universal technical solution may break their code and become a form of "digital licensing". This would also create an unreasonable barrier for entry and innovation thereby hurting internet users.

3. There are also limitations to an audit based system in which users have little recourse or remedy. Here a mix of proactive reporting requirements such as transparency reports and data breach notification requirements, enforcement and adjudication forums are measures which may safeguard user interest.

4. We recommend a, "privacy by design" principle in which each specific technical product, online service and application adopts a set of legal and technical controls. This can be better administered by an independent data protection authority or a privacy commissioner.

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?

Answer summary: TRAI mission is to advance connectivity and the data protection rights of users vis-a-vis telecom. Even as per it's preamble at best its function is limited to, "promote and ensure orderly growth of the telecom sector". Hence, at best it can look at the problems of the telecom sector rather than go into promoting data-focused business models that inhere risks of data protection and user privacy.

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?

Answer summary: *See answer to Question No. 5.*

Question 7: How can the government or its authorized authority set-up 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?

Answer summary: *We are gravely concerned with the framing of the consultation paper which seeks to advocate for a technology based "solution" to safeguard user privacy and data protection. Any technology based solution should be individualised to a product adhering to principles of, "privacy by design" and not operate as a general layer such as a, "consent layer" or the, digilocker technology framework. For further detail see answer to Question No. 4.*

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?

Answer summary: *The safety of communications and digital security is improved by inviting greater penetration testing and allowing independent research.*

1. The safety of communications and digital security is improved by inviting greater penetration testing and allowing independent research. For instance, the declaration of a critical information infrastructure would automatically lead to criminalising any authorised access under Section 70 of the Information Technology Act. This has the potential to negatively affect vulnerability research in systems where such testing is sorely needed.

2. At present even reporting on data breaches by technologists has invited notices from statutory authorities such as the UIDAI which highlights the need for bug bounty program for TSPs or at the very least an established method to strengthen and preserve the safety and security of telecommunications infrastructure. We urge the TRAI to deepen its engagement with information security technologists and network engineers, and ensure that they can conduct penetration testing to improve security in the telecom sector.

3. We are also constrained to point out that the insistence on mandatory linkage of Aadhaar with Mobile which has been issued as per a circular of the DOT after deliberations with TRAI exposes mobile users to greater risk. There are several documented risks of the Aadhaar system and prior to a consultation undertaking or a technical study such a mandatory linking opens users to risk of identity fraud, financial theft as well as surveillance.

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?

Answer summary: *A comprehensive data protection law enforced by an independent data protection authority that has investigatory and enforcement powers is the best mechanism to protect data pertaining to the collection and use of data.*

1. TRAI is a statutory authority established by the TRAI Act and lacks the jurisdictional ability to determine norms for content and application service providers. Specific reference here is made to Sections 11 and 13 of the TRAI Act. Section 13 of the limits the ability of TRAI to, “issue such directions from

time to time to the service providers". Here, "other stakeholders in the digital ecosystem", would fall outside TRAI's jurisdictional ambit.

2. We recognise the need to have a stringent user protection for their data that is collected and used by content and application service providers for which we urge the TRAI to take steps to support a comprehensive data protection law. In the interim it must explore methods through which service providers (TSPs), observe their existing obligations under the TRAI Act and the UAS License. We further call for reform on the prohibition of use of bulk encryption as is presently contained in Clause 37.1 of the UAS license.

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?

Answer summary: *The existing norms applicable to TSPs and other communication service providers are deficient. In addition to the development of robust data protection regulations their horizontal applications needs to be observed with respect to privacy principles which may then be determined by individual adjudications by a data protection authority or a privacy commissioner. We would urge the TRAI to at present, in the interim commence a request for information on the specific practices undertaken by TSPs to ensure compliance with Clause 37 of the UAS License Agreement.*

1. That the consultation paper specifically in Para 2.6 lists several requirements under the Telegraph Act and the UAS license with respect to TSPs. Notably these include, "ensure the protection of privacy of communication and to ensure that unauthorised interception of message does not take place" [Clause 37.2]. The UASL license further contains a prohibition against the deployment of bulk encryption [Clause 37.1] which can lead to practices such as deep packet inspection.

2. Hence not only are the conditions under the Telegraph Act and the UASL license deficient but they also undermine the data protection of users. Hence, the extension of the present regulations to "comparable services"

such as internet based voice and messaging services would undermine user privacy and data protection. This would undermine the very purpose of the present consultation.

3. Parity in principles of data protection and privacy should be maintained horizontally between state and private entities. Further comparable protections should be granted to internet users that should have the powers to adjudicate and apply such principles as per precedent. We would urge the TRAI to at present, in the interim commence a request for information on the specific practices undertaken by TSPs to ensure compliance with Clause 37 of the UAS License Agreement.

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?

Answer summary: *Mass surveillance is illegal and unconstitutional. It has no backing of law and violates the safeguards laid down by the Hon'ble Supreme Court in the telephone tapping case. With respect to individual interception several additional safeguards need to be adopted including promoting secure, encrypted communications.*

1. That telephone tapping and hence interception has been permitted by the Hon'ble Supreme Court after laying down extensive safeguards in the case of *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301. It is relevant to notice that such safeguards which were subsequently incorporated under Rule 419-A of the Telegraph Rules. It is important to recognise that the primary safeguard envisaged were individual interception orders based on the objective assessment of a government functionary. Even this safeguard has come under critique as being non-transparent and being issued mechanically. This has lead to several suggestions to strengthen safeguards as suggested in the Justice A.P. Shah Committee report including notification of the order of interception, to the subject of interception when the interception ceases. We also hope that greater promotion of encryption technologies is suggested to improve data and communications security.

2. It is evident that individualised tapping orders form an important limitation in permissible forms of interception. However we are distressed to note as recently noted by Privacy International in a India specific report that, "[t]hese schemes involve mass interception of communication….they suggest that the Indian state is moving towards large-scale monitoring of its population" [link].

3. This not only conflicts with the 1996 PUCL judgment but the more recent 9 judge bench Puttaswamy decision of the Hon'ble Supreme Court which underscores the need for (a) legality : at present mass surveillance is carried out in the absence of any underlying law; (b) need and a legitimate state aim : which cannot in any instance be a perpetual search warrant on citizens; and (c) proportionality : surveillance the entire population to ensure greater security is *prima facia* offensive to any principle of proportionality. We call on the TRAI to as per it's mandate commence a consultation on the functioning of the interception regime and whether there are adequate to safeguards to protect the privacy of citizens and that no mass surveillance is taking place

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 ?

Answer summary: *Cross-jurisdictional data flows are a complex subject. They may even require an adequacy assessment of a third country which should be done by a data protection authority.*

1. As stated at several portions of our answers we would restate the preference to a comprehensive data protection framework rather than a silos driven approach as is being attempted by the TRAI. While it should act to enforce compliance with existing license conditions and also take steps to halt of any mass surveillance in India as per its mandate under the TRAI Act *et al*, it should to further strengthen the consultation, composition and transparency of the Justice Srikrishna Committee which will frame a comprehensive data protection law.

2. The complexity of the cross-jurisdictional data arise as to, (a) the development of a regulation prohibits data transfers unless certain thresholds of safety are met; (b) for instance such a threshold may include after a review and assessment the grant of an “adequacy status” to the site (usually a foreign country) of data export; (c) the implementation of safeguards prior to export; (d) the enforcement of legal regulation. This may be drawn from the GDPR [link] which may provide as an influential model for cross border flows. It is pertinent to mention that the GDPR which is a recent legal text on data protection will serve and govern data transfers from the European Union places an emphasis on a rule based framework to grant users control and accountability over their personal data.

3. We restate that due to the complexity of not only the development of rules but also due the need of an expertised body to ensure certifications of third countries. Such functions may not only be outside the jurisdictional scope of the TRAI but even beyond it’s mandate and expertise. User interest in such instances may be better served by an independent, expertised Data Protection Authority or a Privacy Commissioner.