INTERNET FREEDOM FOUNDATION

internetfreedom.in policy@internetfreedom.in +91 011 4143 7971

By Email/ Post

To,
Shri Sanjeev Kumar Sharma,
Advisor (Broadband and Policy Analysis),
Telecom Regulatory Authority of India,
Email: advbbpa@trai.gov.in
CC: jtadvbbpa-1@trai.gov.in, jtadvbbpa-3@trai.gov.in

Dated: February 22, 2022 IFF/2022/009

Dear sir,

Re: Counter Comments on "Regulatory Framework for Promoting Data Economy Through Establishment of Data Centres, Content Delivery Networks, and Interconnect Exchanges in India"

1. Internet Freedom Foundation (IFF) is a registered charitable trust which advocates for people's rights over the internet across public institutions and the private sector. IFF's origins stem from the SaveTheInternet.in. This public movement enabled more than a million Indians to advocate that net neutrality be recognised as a core tenet of the public internet.

2. Based on our past engagement with the authority on issues both of net neutrality and informational privacy, we made specific submissions (IFF/2022/007) with justifications for queries related to data monetisation in respect of data centres, Content Delivery Network (CDN) regulation, and informational privacy specifically with respect to the Data Empowerment and Protection Architecture (DEPA). To our dismay, we have noticed the comments posted in response to the present consultation argue in favour of a 'light-touch' regulatory framework for CDNs as well as data monetization, with scant attention paid to regulatory oversight over data privacy and security. These have primarily been made by telecom operators.

3. In our counter comments, we highlight the submissions of service operators,who have largely shirked away from the responsibility of protecting consumer data, and pushed for minimal regulation. This would harm data protection and privacy, especially when the authority considers data digitization proposals. Hence, we would like to restate our recommendations at the same time on the role of the TRAI for strengthening privacy protection. This role can be positively carried out by TRAI in the telecom sector.

We request you to see below the substantive recommendations separately attached to this covering letter. We remain at your disposal should you wish to discuss the matter further.

Sincerely,

Apar Gupta
Executive Director
Internet Freedom Foundation
apar@internetfreedom.in

INTERNET FREEDOM FOUNDATION
internetfreedom.in policy@internetfreedom.in +91 011 4143 7971

Counter Comments on TRAI's Consultation Paper on Regulatory Framework for Promoting Data Economy Through Establishment of Data Centres, Content Delivery Networks, and Interconnect Exchanges in India

Outline of the present submission

Our submission is branched into three broad headings for convenience and consideration. Each section is a specific cluster of questions highlighting an overarching theme along with our comments and recommendations on the issue. These are namely,

- Response on Content Delivery Networks
- Data Ethics - Privacy, Ownership and Security
- Response on Data Monetization

Before we proceed with these issues, we would like to commend the intent towards improving India's digital infrastructure. As the digitalisation of the Indian economy continues, facilitating stronger data protection and net neutrality practises is vital, especially after the online fillip seen during the COVID-19 pandemic. In this regard, focusing on citizens' digital rights while drafting any data-related policy is paramount. Private and state financial incentives, and ease of governance should not sway policy makers into drafting proposals that may pose a risk to user security.

Our comments to the TRAI's Consultation Paper on "Regulatory Framework for Promoting Data Economy Through Establishment of Data Centres, Content Delivery Networks, and Interconnect Exchanges in India" were threefold. First, we called for urgency in the creation of a multi-stakeholder body for the enforcement of net neutrality. Second, we cautioned against regulating CDNs given existing market efficiency and user benefits. Lastly, we urged TRAI to recast focus towards telecom companies practises for data protection standards rather than adopting flawed technical systems of consent (eg. DEPA).

Below we provide our counter comments to responses given by service providers.

INTERNET FREEDOM FOUNDATION
internetfreedom.in policy@internetfreedom.in +91 011 4143 7971

1. Response on Content Delivery Networks

Q28: *What long term policy measures are required to facilitate growth of CDN industry in India?*

Q29: *Whether the absence of regulatory framework for CDNs is affecting the growth of CDN in India and creating a non-level-playing field between CDN players and telecom service providers?*

Q30: *If answer to either of the above question is yes, is there a need to regulate the CDN industry? What type of Governance structure should be prescribed? Do elucidate your views with justification.*

Service Provider	**IFF Comments**
ISPAI: Strongly recommend that a light touch regulatory framework having registration mechanism in place for CDN services should be introduced which would help in creating level playing field for local CDN players. **COAI:** Believe that there should be some framework to govern quality of services provided by CDNs of unlicensed entities. **BIF:** One of the most significant drivers will be the increased use of video data (more cameras everywhere) and the improved resolution of image sensors…(Regulation) should be 'light-touch' so that it permits innovation to prosper but at the same time the Regulator may be permitted to intervene whenever required to take corrective measures in case of market failure, lack of adequate competition, perceptible consumer uneasiness and potential harm so that it acts	We caution against the recommendation put forward by various industry bodies such as Internet Service Providers Association of India and Broadband India Forum of a 'light touch' regulatory framework for CDN service providers. Here, we would like to restate our submissions for further data to be queried to check for anti-competitive practices in the CDN market, especially when the telecom market displays oligopolistic tendencies with three players, namely Reliance Jio, Bharti Airtel and Vodafone Idea, dominating the market.[1] Additionally, if there is an information asymmetry on the nature of how the peering and transit ecosystem functions and the commercial agreements signed between Telecom Service Providers (TSPs) with private parties, the TRAI should put in place a reporting mechanism for TSPs. This should include regular disclosure of privately negotiated interconnection agreements and paid peering/transit arrangements. Pursuant to this, once adequate studies of the market have been conducted to make robust assessment, TRAI can facilitate the growth of

[1] Telecom Regulatory Authority Of India, *Highlights of Telecom Subscription Data as on 30th June, 2021,* https://www.trai.gov.in/sites/default/files/PR_No.37of2021_0.pdf

as a deterrent instead of a market barrier. **Reliance Jio Infocomm:** Recommend that CDNs should be brought under a regulatory framework so that the contractual arrangements between internet companies, CDNs and TSPs/ISPs can be monitored for any anti-competitive practices and violation of any net neutrality principles. Hence CDNs should be brought under suitable licensing regime, with light touch regulatory approach. **Tata Communications:** We strongly recommend that a light touch regulatory framework having registration mechanism in place for CDN services should be introduced which would help in creating a level playing field for local CDN players. **Bharti Airtel:** We believe that commercial arrangements between CDN and ISPs should continue to be governed by market forces, and no regulatory intervention is required in the same. It is necessary to put some obligations on CDNs, operated by unlicensed entities, for maintaining minimum quality of standards. **Vodafone Idea:** There should be a clear legal and regulatory regime for CDN industry through light touch licensing regime.	the local CDN industry by formulating a non-regulatory policy focussing on technology promotion and incentives. Further, we commend the authority for its recommendations to create a multi-stakeholder body for enforcement of net neutrality, primarily technical forms of discrimination that the Unified Access Service Agreements prohibit. However, we express regret at the delay in establishing this multi-stakeholder body which is to the detriment of India's global leadership on net neutrality. Furthermore, on 24th September, 2021, the Ministry of Finance (vide O.M.F.No.12(13-B(W&M)/2020) has removed the expenditure curbs that were imposed on various Ministries/Departments due to COVID-19 related austerity measures.[2] Thus, curbs on expenditure have now been removed and so COVID-19 related budgetary cuts can no longer stand in the way of the implementation of TRAI's recommendations. We are already seeing increasing instances of licensees discriminating against certain types of internet content and blocking them with impunity. As we had pointed out in our comments, website blocklists of licensed internet service providers (ISPs) across India are widely inconsistent with one another, suggesting that a larger pattern wherein internet providers are either a) not complying with blocking orders, or b) arbitrarily blocking websites without legal orders.[3] This undermines the network neutrality principles, Unified Access Service Agreements, and the spirit of the Supreme Court of India's

[2] O.M.F.No.12(13-B(W&M)/2020). Ministry of Finance. Notified on 24th September, 2021. https://dea.gov.in/sites/default/files/Cash%20Management%20Guidelines-24-9-21.pdf.

[3] Singh, Grover & Singh, *How India Censors the Web*, Cornell University, 30th May, 2020; https://arxiv.org/abs/1912.08590

SugarBox Networks: We advocate non-disclosure of commercial terms of a strategic partnership to keep the CDN industry profitable and competitive…We propose a suitable protection mechanism that hedges the business risk of CDN service providers from peering disputes of any such kind.	directions in *Anuradha Bhasin v. Union of India and Ors, Writ Petition (Civil) No. 1031 of 2019* mandating transparency in internet restrictions. Thus, it is imperative that the multi-stakeholder body be constituted to fulfil the following tasks: 1. Help to conduct a comprehensive study of the CDN market with inputs from diverse stakeholders 2. Audit TSPs to ensure non-deployment of undue traffic management practices. 3. Ensure transparency in the sector by publishing regular reports of multistakeholder discussions Lastly, as we note the growth in the CDN industry, we should be watchful of the technology that is abetting the growth. In this light, it is unfortunate to note the response of the Broadband India Forum, which effectively rationalises the deployment of cameras for infrastructural purposes. While video data generated through OTT platforms is permissible, deploying cameras everywhere for surveillance purposes is dangerous. Any data protection law should limit mass surveillance as it contravenes the principles of necessity, proportionality and purpose limitation. Even when individual interception and surveillance is carried out, it should be severely limited in substance and practice through procedural safeguards. As we await data protection legislation, TRAI should ensure that private companies do not resort to data maximisation, lest it contravenes the *Justice KS Puttswamy v. Union of India* judgement .[4]

[4] 2017 (10) SCC 1.

2. Response on Data Ethics - Privacy, Ownership and Security

Q47: *How can the TSPs empower their subscribers with enhanced control over their data and ensure secure portability of trusted data between TSPs and other institutions? Provide comments along with detailed justification.*

Q48: *What is the degree of feasibility of implementing DEPA based consent framework structure amongst TSPs for sharing of KYC data between TSPs based on subscriber's consent?*

Service Provider	**IFF Comments**
COAI: At present, data protection regulations are not equally equipped for different sectors to maintain the security of personal data in control of the data fiduciary in the sector. Hence implementation of DEPA cannot be done simultaneously for all the sectors…Recommend a distributed ledger managed by a consortium with a consistent taxonomy. This can have subscriber details, log of access and usage. This approach will balance privacy and control. **Reliance Jio**: At present, data protection regulations are not equally equipped for different sectors to maintain the security of personal data in control of the data fiduciary in the sector. Hence implementation of DEPA cannot be done simultaneous for all the sectors…Although it should be explicitly mentioned that the liability of maintaining the security of shared data lies with the Consent Manager, as it is the entity obtaining user consent for sharing of his/her data. Role of TSPs will be limited to providing the	IFF commends COAI and Reliance Jio's acknowledgment of India lacking data protection regulations for different sectors to maintain the security of personal data. TRAI should focus on TSPs and improve the privacy and data protection standards applicable to them in the interim till a comprehensive data protection law is enacted. As answered by the Minister of State for Communications Devunsinh Chauhan in the Rajya Sabha, the DoT has not reviewed the privacy policy of TSPs in India, and that the department has not imposed any fines on TSPs for violation of the Information Technology Act, 2000 and the Information Technology Rules, 2011.[5] This is concerning since as per media reports personal data, including names, birth date, phone number, address and Aadhar IDs of over 2.5 million Airtel subscribers, were available on a hacker group's website for about three months last year.[6] Similarly, in 2019, an independent security researcher

[5] Department of Telecommunications; *Rajya Sabha Unstarred Question No. 386- Review of Privacy Policy of Telecom Service Providers*; February 4th, 2022; https://pqars.nic.in/annex/256/Au386.pdf

[6] Chandrashekhar, Mittal; *Airtel denies claims that data of 2.5 million users was leaked*; February 3rd, 2021; https://economictimes.indiatimes.com/tech/technology/airtel-denies-claims-that-data-of-2-5-million-users-was-leaked/articleshow/80660207.cms?from=mdr

requested data, on being provided the appropriate consent, on behalf of the user to the Consent Manager, as such data is already available with the TSPs in digital format. **Tata Communications:** For any laps /non-compliance regarding sharing of KYC data without the consent of subscriber, existing TSP who has possess the KYC information of the Subscriber should not be held responsible in any manner **Bharti Airtel:** The recommended approach is a distributed ledger that is managed by a consortium with a consistent taxonomy. This has subscriber details, log of access and usage. This approach balances privacy and control.	exposed a flaw in the Application Programming Interface of Airtel's mobile application, which could have exposed data of 300 million users.[7] Hence, there is a need for stricter enforcement of data protection measures and a penalty imposition in case of violation. Additionally, the usage of telecom user data and its commercial exploitation needs to be studied. Disclosures may be mandated till the enactment of a user centric, rights respecting data protection law that provides for horizontal regulation. One of the core principles of such a data protection law may include interoperability and data portability. A citizen oriented framework can only emerge on the basis of centering data exchanges within a framework of data protection that recognises and corrects the power differentials between data principles and processors. Taking a cue from the GDPR, TRAI should ensure that the consent taken is valid, and indeed, informed.[8] This is paramount to ensure that citizens' rights over data are maintained. However, TRAI should keep in mind the implementation challenges of obtaining informed consent before going ahead with the DEPA framework. Millions of Indian citizens possess low levels of education, with digital literacy being a distant dream. In such a context, most users would be incapable of giving their consent truly freely. Unaware of their rights as users and citizens, they may not fully comprehend the implications of consenting to sharing their data, thus risking a breach of privacy and security. Further, Reliance Jio and Tata

[7] ibid

[8] GDPR: Consent, Intersoft Consulting, accessed November 28th, 2020; https://gdpr-info.eu/issues/consent/

	Communications in their present submission argue that the liability of maintaining the security of shared data lies with the Consent Manager, limiting the role of the TSPs to just being the provider of the data. This demand presupposes the robust technical and legal ability of the DEPA to ably protect user data even though the framework is not anchored under a legal framework providing enforceable rights and remedies to end-users. Moreover, the telecom data-sharing framework laid out in the Consultation Paper neither specifies the parties with whom telecom data can be shared nor does it refer to a regulatory authority that will have the power to identify parties with whom such information will be shared. It is unlikely that users will have enhanced control of their data if they do not have the power to decide who gets to access their data.

3. Response on Data Monetization

Q27: *Would there be any security/privacy issues associated with data monetization? What further measures can be taken to boost data monetization in the country?*

Service Provider's Submissions	**IFF Response**
COAI: Presently there is adequate regulatory oversight to ensure data privacy and data security of customer data as well as customer communication for the licensed service providers… Businesses should get explicit recognition that anonymous data is not personal data and that pseudonymisation can provide genuine safeguards without the need for consent.	Any government policy that promotes "data monetisation" based on public data should be cautioned against it. Such policies will encourage state authorities to collect data beyond the specified purpose, leading to data maximisation. This will conflict with citizens' fundamental right to privacy and the principle of data minimisation as recognised by the Supreme Court of India in the *Justice KS*

	Puttaswamy v. Union of India.[9]
Reliance Jio: Select data digitization drive can be undertaken for domains/industries which are well placed for secure processing of the data. Government departments should take a lead in this and be the pioneers in digitization of hard documents already in possession of various Reliance Jio Infocomm Ltd departments. They can develop the infrastructure and framework for secure processing of such digitized data.	Moreover, in the absence of a data protection law, data monetization will undoubtedly result in actual harm for citizens with little to no legal recourse. IFF disagrees with COAI's statement arguing India has adequate regulatory oversight to ensure data privacy and security of customer data. In February 2020, reports emerged that a vehicle database developed by the Ministry of Road Transport and Highway (MoRTH) called Vahan, was being misused by rioters for purposes of targeted violence as it was accessible by third parties and the public.[10] Although the data was later recalled, it exposed the privacy risks that could emerge from allowing public access to such information.[11] Such unfettered sharing of data, without appropriate consent mechanism or legal/institutional safeguards, can threaten the security and fundamental freedoms of minority and at-risk groups.
Bharti Airtel: Suggest to create authorised centers for digitization wherein current infrastructure (Aadhaar kiosks, payments bank kiosks) could be used to digitize documents for the citizen. To take care of security and privacy related concerns, an authorization/alerting mechanism should be put in place when a citizen's data is accessed e.g. message alerts and information of agency/ enterprise accessing the information…In addition, businesses should get explicit recognition that anonymous data is not personal data and that pseudonymization can provide genuine safeguards without the need for consent…We submit that, presently there is adequate regulatory oversight to ensure data privacy and data security of customer data as well as customer communication for the licensed service providers.	Further, caution should also be taken while processing anonymised data. Service providers, like COAI and Bharti Airtel in the present consultation paper have said "businesses should get explicit recognition that anonymous data is not personal data and that pseudonymization can provide genuine safeguards without the need for consent". However, this demand fails to satisfy data privacy norms on two grounds. First, it isn't easy to ascertain what data constitutes personal or non personal data (NPD).

[9] 2017 (10) SCC 1.

[10] Internet Freedom Foundation; *We have written to Government asking them to stop public access to the Vahan database #SaveOurPrivacy*; February 26th, 2020; https://internetfreedom.in/we-have-written-to-government-asking-them-to-stop-risks-of-misuse-of-government-datasets/

[11] Internet Freedom Foundation, *MORTH scraps bulk data sharing policy*; 30th June 2020 https://internetfreedom.in/morth-bulk-data-sharing-policy-scrapped/

	International opinion on such issues has generally strayed towards a more robust definition of NPD. For example, the European Court of Justice has held that even for data points that are not sufficient in and of themselves to identify a data subject (such as dynamic IP addresses), "such a piece of information has to be treated as personal data provided that the missing pieces of the puzzle can also be collected by other sources".[12,13] Second, the ease with which de-anonymisation of data can be conducted must be accounted for. Several studies have indicated the increased threat of de-anonymisation, both directly and indirectly. Direct attacks through decryption may, for example, "successfully identify users' Netflix records, uncovering their political preferences and other potentially sensitive information."[14] Meanwhile, indirect 'inference' attacks use already available data "to deduce new personal information not explicitly present in the original data".[15] The real-world effects of these attacks have already been demonstrated. One study showed that just 4 data points about mobile phone location could uniquely identify 95% of the test population.[16] Another study showed that just three transactions are enough to identify an

[12] Marda; *Non-personal data: the case of the Indian Data Protection Bill, definitions and assumptions;* October 15th, 2020; https://www.adalovelaceinstitute.org/blog/non-personal-data-indian-data-protection-bill/

[13] Aryan; *Explained: What is non-personal data?;* The Indian Express, July 27th, 2020; https://indianexpress.com/article/explained/non-personal-data-explained-6506613/

[14] Lee, Liu, Ji, Mittal, & Lee; *Quantification of De-anonymization Risks in Social Networks*; Princeton Architecture Laboratory for Multimedia and Security, March 15th, 2017; http://palms.ee.princeton.edu/system/files/Quantification+of+De-anonymization+Risks+in+Social+Networks.pdf.

[15] Gambs, Killijian, & del Prado Cortez; *De-anonymization attack on geolocated data*; Journal of Computer and System Sciences, April 18th, 2014; https://www.sciencedirect.com/science/article/pii/S0022000014000683.

[16] Zyga; *Study shows how easy it is to determine someone's identity with cell phone data*; Phys.org, March 25th, 2013; https://phys.org/news/2013-03-easy-identity-cell.html.

	individual's credit card.[17] Hence, it is advisable to wait for the passing of the data protection law before the government embarks on a data digitization drive. This will not only protect citizens' digital rights, but also ensure robust regulatory mechanisms for both personal and non-personal data.

[17] Kirk; *How three small credit card transactions could reveal your identity*; January 25th, 2015; https://www.computerworld.com/article/2877935/how-three-small-credit-card-transactions-could-reveal-your-identity.html.