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

By Email

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

Dated: February 10, 2022 IFF/2022/007

Dear sir,

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

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 the Regulatory Framework for Promoting Data Economy Through Establishment of Data Centres, Content Delivery Networks, and Interconnect Exchanges in India.

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

1. **Advocates for a rights based informational privacy law:** Public campaigns and legislative engagement 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 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 practises as well as called for interim orders to protect the interests of our fellow citizens [link]. It has also filed an information request with the Competition Commission of India against Whatsapp.

3. **Regulatory engagement to protect user privacy and net neutrality:** Participation in past TRAI consultations where we have highlighted the urgent need to protect user privacy and net neutrality, including:
    a. Response to Privacy, Security and Ownership of the Data in the Telecom Sector Consultation [link]
    b. Response to Traffic Management Practices (TMPs) and Multistakeholder Body for Net Neutrality Consultation [link]
    c. Supplementary submission to Traffic Management Practices and a Multistakeholder Body for Net Neutrality Consultation [link]

Based on our past engagement with the authority on issues both of net neutrality and informational privacy, we have made specific submissions with justifications for queries related to data monetisation in respect of data centres, CDNs and informational privacy specifically with respect to the Data Empowerment and Protection Architecture (DEPA). We hope the TRAI takes forward the specific suggestions made by us against each of its queries.

Sincerely,

Apar Gupta,
Executive Director,
Internet Freedom Foundation

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

Comments to the Consultation Paper on Regulatory Framework for Promoting Data Economy Through Establishment of Data Centres, Content Delivery Networks, and Interconnect Exchanges in India

Response on Data Centres

Question 26: What institutional mechanism needs to be put in place to ensure digitization of hard documents within a defined timeframe?

Answer Summary: *As digitization increases at a fast pace, it is important to first safeguard for data privacy and provide for user consent. Second, India's lack of robust infrastructure needs to be taken under consideration while pushing for implementation of digitization, lest the harms outweigh the benefits. With a wide digital divide in the country, digitization should be implemented in a phased manner with incentives being given to smaller institutions to further push them to adopt digital solutions. Third, given that digitisation of documents is properly administered through provisions under the Information Technology Act, 2000 and to be administered by MEITY the TRAI may exercise forbearance to avoid inconsistency.*

1. To substantiate the answer provided above we are utilising the rapid digitisation in health data.. There has been a rapid rise in telemedicine and eConsultations prompted by the Covid-19 pandemic. For example, as of 4th October, 2021, the Union Government's telemedicine initiative completed 1.34 crore consultations, with 80.33 lakh doctor-to-doctor consultations and 53.78 lakh patient-to-doctor consultations.[1] Thus, it is likely that even smaller private clinics are likely to adopt some form of digitisation. As a result, it is important to ensure that as and when public and private sector institutions digitise, adequate safeguards for data protection through a user centric, rights respecting legislative framework that creates a regulatory body for enforcement. This should form as the first step in any comprehensive plan for digitisation.

2. However, a comprehensive digital system can only be built on the back of robust infrastructure, something India may lack at present. Pushing the implementation of digitization without adequately taking into account and planning for these requirements will cause more harm than any stated benefit of digitization. It will most likely result in harms such as exclusion and denial of services. As an issue this needs to be considered beyond tele connectivity and smartphone usage to specific use cases. For instance, a NITI AAYOG report has stated that nearly 33% patients who get admitted in private

[1] Ministry of Health & Family Welfare; Health Ministry's eSanjeevani Completes 1.3 Crore Consultations (Release ID 1760862); Press Information Bureau; 4th October, 2021; https://pib.gov.in/PressReleasePage.aspx?PRID=1760862

hospitals in India go to nursing homes manned by just one healthcare worker[2]. Some studies, evaluating existing electronic health record (EHR) systems in India, find several deficiencies particularly in relation to the quality of data being recorded. For example, a 2016 study on EHR systems for maternal and child health care in Haryana found the quality of data to be sub-optimal with over-reporting in certain indicators and missing data in other indicators.[3] A 2018 study on MCTS in a district in Orissa, identified poor internet connectivity, incomplete data entries, underreporting, discrepant reporting and inefficient monitoring as some of the factors leading to the poor functioning of the Mother Child Track System.[4] In light of such concerns, alongside the general 'digital divide' that pervades the country, it is imperative that the policy is implemented in a phased manner in which all government facilities that lack the infrastructure or capacity to digitise are provided support through grants by rural and urban local bodies.

3. Finally, one of the central objectives of the Information Technology Act, 2000 has been to provide legal recognition to electronic records. The legislation further contains a distinct chapter on e-governance and specific provisions for digitisation of records. For instance under Section 6(2) it provides that, "the manner and format in which such electronic records shall be filed, created or issued". Given this law, as well as the aforementioned online portal is administered by the Ministry of Electronics and IT, to avoid inconsistency in policy, the TRAI may exercise forbearance in this matter, especially with regard to mandating timelines for digitisation.

Question 27: Would there be any security/privacy issues associated with data monetization? What further measures can be taken to boost data monetization in the country?

Answer Summary: We submit strong concern on any government policy that promotes, "data monetisation" premised off public data. This will prompt a revenue incentive for state authorities to collect more data than necessary for specified purposes. It is likely to conflict with the fundamental right to privacy and in the absence of a functional data protection law will certainly result in real harm and risk for citizens of India.

---

[2] *Health Systems for a New India: Building Blocks—Potential Pathways to Reforms*; NITI Aayog; 18th November, 2019; https://www.niti.gov.in/sites/default/files/2019-11/NitiAayogBook_compressed_1.pdf

[3] Sharma et al; *Quality of Health Management Information System for Maternal & Child Health Care in Haryana State, India*. PLoS ONE 11(2): e0148449; February 2016; https://pubmed.ncbi.nlm.nih.gov/26872353/

[4] Dehury & Chatterjee; *Assessment of health management information system for monitoring of maternal health in Jaleswar Block of Balasore District, Odisha, India*. Indian J Public Health, 62; December 2018; https://pubmed.ncbi.nlm.nih.gov/30539886/

1. The economic objectives of prompting economic value through greater amounts of data collection, especially personal data or sensitive personal data presents substantial risk. For three primary reasons. The first is that a strong fiscal temptation for the government through sale or commercial exploitation prompts a perverse incentive. For instances of commercialisation of state data for greater amounts of data collection. Such activity will result in data maximisation which will conflict with a core principle of data protection which limits collection by a data processor to the purpose for which it is collected. Here, this principle of data minimisation has also been recognised by the Supreme Court of India in the fundamental right to privacy judgement, *Justice KS Puttaswamy v. Union of India*[5].

2. The second reason is for the well documented basis to injury that may result to individuals on the basis of prior government experience. Here, the specific example of the commercialisation of the VAHAN (vehicular registration) and driver's licence is useful. Initially sold to private service providers by the Ministry of Road, Transport and Highways it was recalled after privacy risks emerged that could result in injury to individuals and property.[6]

3. The third reason is the absence of data protection law, or a regulatory body to enforce it. At present the Data Protection Bill, 2021 as recommended by the Joint Parliamentary Committee has yet to attain the status of law. It is further expected that there may be some transitory periods for enforcement, especially the allocation of resources and personnel for the proposed Data Protection Authority. In their absence any person is left without recourse and remedy. Further, private and state service providers who collect and process personal data do not have clear, brightline rules to enforce within their operations and business practises. In such a legislative vaccum it would be perilous to adopt a policy for data maximation.

<u>Responses on Content Delivery Networks</u>

Question 28: What long term policy measures are required to facilitate growth of the CDN industry in India?

Answer Summary: At present there exists little evidence of lack of market failure in CDNs warranting maintaining the authority's past determination of adopting a policy of forbearance.

[5] 2017 (10) SCC 1.

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

Such data and evidence based policy prescriptions may be commenced as to any *information asymmetry regarding interconnection agreements of TSPs based on disclosure compliances from TSPs. In the interim, net neutrality principles need to be safeguarded by prohibiting ISPs from extracting toll charges and intentionally creating slow and fast lanes. A multi-stakeholder enforcement body, as recommended by the TRAI is yet to be created. This would provide a more informed, evidence based policy determination on the issue.*

1. Internet traffic volumes are continuously rising, especially driven by video streaming services. The Economic Survey 2021-22 revealed that India's average data usage has increased from 1.24 GB per month in 2018 to 14.1 GB in June 2021.[7] As internet usage increases, this may pose an outcome of past trends as analysed by BEREC holding during much more recent years. It states that prices for transit or CDN services are declining, indicating that the market is highly competitive but at the same time under pressure, both from peering services and CDN services.[8] Hence, the importance of CDNs as a means of traffic delivery coincides with the general growth in internet traffic. Here, there needs to be a cautious restraint exercised by the authority towards proposals for any ex-ante regulation on CDN providers.

2. At present there exists little evidence of lack of market failure in CDNs warranting maintaining the authority's past determination of adopting a policy of forbearance. As BEREC has determined CDN markets are working adequately and disputes that arise due to traffic asymmetries are often resolved mutually between the parties[9]. Hence, in order to facilitate growth of the local CDN industry rather than regulating existing CDN providers a non-regulatory policy may be formulated focussing on technology promotion and incentives. In the interim to determine the anti-competitive effects if any a detailed, evidence based study is necessary given that the CCI's report Market study on the Telecom Sector in India - Key Findings and Observations' dated 22nd January 2021 itself is based on press reports and opinion pieces. Hence, prior to formulating a view on the subject specific data that may be queried from TSPs under disclosure norms may be commenced by the authority.

3. At present, there is potential for TSPs to abuse interconnection agreements to violate net neutrality principles. However, we lack enough information to suggest exact policy

[7] TeamInc42, '*Economic Survey 2022: India's Internet Data Usage Shoots Up To 14.1 GB Per Month',* 31 January, 2022; https://inc42.com/buzz/indias-internet-data-usage-shoots-up-to-14-1-gb-per-month/

[8] BEREC, *BEREC Report on IP-Interconnection practises in the Context of Net Neutrality,* 5 October, 2017; https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/7299-berec-report-on-ip-interconnection-practices-in-the-context-of-net-neutrality#:~:text=In%202012%20BEREC%20published%20the,patterns%20and%20in%20business%20models

[9] ibid

recommendations. This information asymmetry arises from the nature of how the peering and transit ecosystem functions. Any commercial arrangement in this space is directly negotiated between private parties with TSPs and remains there, making trend mapping difficult. Hence, TRAI should work towards seeking more information by putting in place a reporting mechanism or a knowledge sharing process for TSPs. This should include regular disclosure of privately negotiated interconnection agreements and paid peering/transit arrangements. In the future, when there's more information available, TRAI may consider regulating based on evidence and trends which emerge from such data after publishing a consultation paper.

4. In the interim, as the number of CDN providers increase, TRAI must ensure that ISPs don't extract toll charges from the content provider and the CDN provider in addition to the payments made by users that subscribe to these ISPs. This will help in the creation of more services that are bandwidth intensive and boost competition at the last kilometre. Lastly, TRAI must also ensure that ISPs cannot restrict CDNs to deliver content that support the ISPs own services or be subject to arbitrary compensation demands. The regulator should see to it that ISPs don't create fast and slow lanes depending on the user payment by intentionally degrading the standard service. This violates the core principle of net neutrality which aims to safeguard open and free internet to all. Here we would commend the authority for it's recommendations for the creation of a multi-stakeholder body for enforcement of net neutrality, especially technical forms of discrimination that are prohibited by the Unified Access Service Agreements. However, we express regret at the delay in the establishment of this multi-stakeholder body which is to the detriment of India's global leadership on net neutrality.

Question 29: Whether the absence of a 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?

Answer Summary: *IFF strongly believes that the internet should be maintained as a free and open platform, on which network providers treat all content and services equally. However, as per trends today, the market size is restricted. As per the authorities regular reports on tele connectivity three TSPs, namely Reliance Jio Infocomm Ltd, Bharti Airtel and Vodafone Idea dominate the broadband service market. Hence, there is a high possibility of non-adherence to net neutrality principles. Hence, we believe there's an urgent need to establish a strong and independent multi stakeholder body to safeguard the open and free internet in India as recommended by the authority. This would promote a level playing field for all CDN players through disclosure norms and the enforcement of principles of non-discrimination.*

1. IFF adopts the definition of net neutrality by Prof. Vishal Misra who provided a definitional framework to the SaveTheInternet.in movement. He states that net neutrality means, "*the Internet be maintained as an open platform, on which network providers treat all content, applications and services equally, without discrimination"*.[10] This includes ensuring that network providers do not supply any competitive advantage to specific apps/services, either through pricing or Quality of Service". These principles have been incorporated within Unified Access Service Agreements and are today applicable to TSPs.

2. As per TRAI's Telecom Subscription Data for June 2021, there is a high amount of market concentration among service providers.[11] As of June 30th, 2021, 95.67% of the all-India market share for broadband services is captured by 3 service providers - Reliance Jio Infocomm Ltd (436.69 million), Bharti Airtel (193.74 million), Vodafone Idea (121.41 million). This creates a risk of oligopolistic tendencies and is likely to have a negative effect on the implementation of net neutrality, as in the lack of a competitive market, dominating players with a high share of the market may not adhere to the values of transparency and accountability.

3. This is further highlighted by the fact that there are increasing instances wherein licensees continue to discriminate against certain types of internet content and block them with impunity. These instances conform with observations from a larger study published by the Centre for Internet and Society, Bangalore (CIS) which was published on January 17, 2020.[12] In it, researchers found that the 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. This undermines the network neutrality principles; Unified Access Service Agreements; and, the spirit of the Supreme Court of India's directions in *Anuradha Bhasin v. Union of India and Ors*, Writ Petition (Civil) No. 1031 of 2019 mandating transparency in internet restrictions. In order to counter such regressive impacts on India's net neutrality regime, a strong and independent multi stakeholder body is of crucial importance.

---

[10] *Is the DoT doing a rethink on net neutrality? We press for transparency and enforcement #SaveTheInternet,* Internet Freedom Foundation, 26th August, 2021; https://internetfreedom.in/is-the-dot-doing-a-rethink-on-net-neutrality-we-press-for-transparency-and-enforcement-savetheinternet/#:~:text=net%20neutrality%20by-,Prof.%20Vishal%20Misra,-who%20states%20that

[11] 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

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

Question 30: If answer to either of the above questions 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.

Answer Summary: *While the nature of a competitive market doesn't call for a need to regulate CDNs, we urge that its impact be monitored through disclosure from TSPs to provide a level playing field for the free and open internet.*

1. CDNs enhance efficiency and quality and hence should be encouraged. Geoff Huston, Chief Scientist at Asia Pacific Network Information Centre (APNIC) said, "*We are now seeing the rapid rise of the content data network (CDN) model, where instead of an Internet carrying the user to a diverse set of content stores, the content stores are opening local content outlets right next to the user. As all forms of digital services move into CDN hostels, and as the CDN opens outlets that are positioned immediately adjacent to pools of economically valuable consumers, then where does that leave the traditional carriage role in the Internet?*"[13].

2. Hence, while it is early to formulate regulation or policy proposals there is a need for deeper, continuing evidence based study. As experts note the growing dominance of CDNs that is almost replacing public internet, it's imperative to keep a watch on their impact. BEREC also believes interconnection services need not come within the scope of regulation as only internet access services provided to end-users need regulation.[14] For further information on the monitoring policies to be implemented, please refer to Answer 28.

Question 31: In case a registration/licensing framework is to be prescribed, what should be the terms and conditions for such framework?

Answer summary: *Prior to drafting a registration framework, TRAI should first ensure the net neutrality principle is mandated on all internet access providers. As we have reasoned before, there is no need for a registration/licensing framework. Instead, we recommend study, data collection and the enforcement of disclosure norms for TSPs.*

1. Drafting any framework for registration or licensing of CDNs should first and foremost keep net neutrality principles in mind. In addition It should be understood within India's proud democratic roots that it requires a plural and diverse Internet. Being a developing nation with a less mature market, we need to ensure that net neutrality is mandated by

[13] Huston, Geoff, *The Internet's Gilded Age,* The ISP Column, March 2017; https://www.potaroo.net/ispcol/2017-03/gilding.html

[14] BEREC, '*What is covered and protected by the regulation',* https://berec.europa.eu/eng/netneutrality/regulation/

regulation to prevent any abuse. We believe this can be achieved within the existing framework of recommendations existing with the authority, specifically it's prior forbearance of regulation for CDNs and recommendations for the creation of a multi-stakeholder body for the enforcement of net neutrality. Such a multi-stakeholder body, working with the authority will be best placed to study the competitiveness of the market and the existence of any market barriers that impact end users through disclosure norms for TSPs.

2. The overall policy approach for regulation needs to be within a constitutional framework as has been adopted by the authority in the past. For instance, the authority in its explanatory note on the Differential Data Pricing Regulations in February 2017 has stated, "… t*he right to express oneself as well as the right to receive information are critical elements in the use of the internet. The Authority is of the view that use of the internet should be in such a manner that it advances the free speech rights of the citizens, by ensuring plurality and diversity of views, opinions, and ideas*".

Question 37: Are there any other issues that are hampering the development of CDN Industry in India? If there are suggestions for the growth of CDNs in India, the same may be brought out with complete details.

Answer summary: *We urge that for the holistic development of CDNs be guided by authentic data around internet shutdowns, COVID-19 impact on internet capacity, internet traffic, CDN price trends.*

1. Even in the period that a multi-stakeholder body is established for net neutrality enforcement, the authority in the meanwhile can adopt certain best practises that lead to data collection and cross-sectoral inputs. For instance, BEREC convenes open meetings twice a week between national regulators, and telecom players to regularly keep track of the impact COVID-19 and lockdown pressures on internet traffic are having on underlying network infrastructure. Based on this authorities have the ability to audit service providers and ensure they do not deploy undue network management practises. Laudably, to ensure transparency BEREC publishes weekly reports of these discussions, how internet infrastructure has been impacted by the current developments, and if any jurisdiction or operator has experienced an anomalous event where the network has had to deal with undue traffic. Until now European authorities have observed that their networks have not been particularly stressed by the surge in home networks and peak traffic during the current health crisis. Along these lines we suggest India should have twice a week meetings between DoT, TRAI, TSPs/ISPs, internet exchange points, CDN providers, cloud service providers, content providers, small businesses, video conferencing app developers, digital rights groups, technologists and academics,

consumer groups and so on, to ascertain the actual impact COVID-19 is having on internet capacity and quality of service.[15]

2. Another, incidental area that deserves consideration are the widespread internet shutdowns that will pose challenges for Indian CDN providers. This is an area that may also merit detailed technical study on the network and economic impact on CDN providers. As per a report authored by Top10VPN, the internet was shut down for 1,157 hours in 2021 in India, costing the economy $582.8 million.[16] In 2020, the internet was suspended for 8,927 hours, more than anywhere else in the world, costing the Indian economy $2.8 billion.[17] In 2019, the internet was suspended in India for 4,196 hours, costing the Indian economy $1.3 billion.[18] This amounts to 14,280 hours of internet suspensions over three years and represents a loss of nearly $4.7 billion.

3. Here, website blocking also poses an issue due to an existing lack of transparency. For instance, in 2019, the government blocked Tanul Thakur's satirical Dowry Calculator website citing provisions of the Dowry Prohibition Act, 1961 which prohibits giving and taking of dowry, and bans individuals from publishing advertisements offering dowry. However, Tanul Thakur's website is clearly inapplicable to this Act as it parodies and mocks the patriarchal practice of dowry rather than glorifying it. Further, as per the Section 69A of the Information Technology Act, 2000 which empowers the government to block websites was upheld by the Supreme Court in the *Shreya Singhal v. Union of India* case because there is a mandatory obligation to provide notice and hearing to the individual before blocking his/her website. However, this is often not the case as witnessed in the Tanul Thakur incident as well.[19] This manifests itself in the non-publication of blocking orders which lead to inconsistent and arbitrary application across TSPs. Here, it would be incorrect to attribute fault to CDNs for facilitating access to blocked content given such orders are not publicly made available.

---

[15] Internet Freedom Foundation, Representation Seeking Actions Toward Internet Access During COVID-19, 24 April, 2020; https://drive.google.com/file/d/1Hn8zB2ZHWxJ1Uf8GgWUDwkIFj-tdgFMl/view

[16] Top10VPN, *Government Internet Shutdowns Have Cost Over $18 Billion Since 2019,* 1 February, 2022; https://www.top10vpn.com/research/cost-of-internet-shutdowns/

[17] Top10VPN, *Government Internet Shutdowns Cost Over $4 Billion in 2020,* 4 January 2021; https://www.top10vpn.com/research/cost-of-internet-shutdowns/2020/

[18] Top10VPN, *Government Internet Shutdowns Cost $8 Billion in 2019,* 3 January, 2020; https://www.top10vpn.com/research/cost-of-internet-shutdowns/2019/

[19] Internet Freedom Foundation, *MeitY defends blocking of satirical Dowry Calculator website #FreeToMeme,* 16 March, 2020; https://internetfreedom.in/meity-defends-blocking-of-satirical-dowry-calculator-website/

Data Ethics - Privacy, Ownership and Security

Question 47: 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.

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 Department of Telecommunication, and penalty provisions must be used to enforce this. Further, their usage of telecom user data and it's commercial exploitation needs to be studied and disclosures may be mandated till the creation 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.*

1. 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. For instance, the GDPR contains many robust measures for ensuring that consent taken is valid and, indeed, informed. It does so to ensure that citizens' rights over their data are held to be of paramount importance, and deals with various complications on the basis of this principle. For example, on the issue of bargaining power differentials, it takes the view that, "*Any element of inappropriate pressure or influence which could affect the outcome of that choice renders the consent invalid. In doing so, the legal text takes a certain imbalance between the controller and the data subject into consideration. Thus, the performance of a contract may not be made dependent upon the consent to process further personal data, which is not needed for the performance of that contract*".[20]

2. The consultation paper notes the various provisions of the Personal Data Protection bill, 2019[21] as well as of the Draft Data Protection bill, 2021[22] which are at best, at present legislative proposals without the force of law. The timeline for its enactment and enforcement that provides real remedy and regulatory governance is indeterminate. Further, the authority must further study the existing proposal for broad carve outs

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

[21] The Personal Data Protection Bill (Bill 373 of 2019); http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

[22] *Report of the Joint Parliamentary Committee on the Personal Data Protection Bill, 2019*; 17th Lok Sabha (pg. 475); 16th Dec, 2021; https://drive.google.com/file/d/1emcAB8HjE2oCC_DI6zR5YPnPQ5iwwwCT/view.

created for processing personal data without user consent that conflict from it's past recommendations on data privacy as much as the present consultation paper. Under Clause 13 of the 2021 bill, any personal data except sensitive personal data can be processed if necessary or reasonably expected by the data principal for purposes related to employment. Under clause 14, personal data can also be processed if necessary for reasonable purposes, which include credit scoring, prevention and detection of fraud, mergers and acquisitions, operations of search engines etc. Such large exceptions can render the very principle of consent meaningless.

3. The paper also notes the rights of the individuals as provided for in the 2019 and the 2021 bill. It must be noted that the exercise of these rights is severely constrained as a result of Clause 18(2) of the bills which allows data fiduciaries to reject requests for correction, completion, updation or erasure of personal data if they disagree with such requests (on the basis that certain data is still necessary for the purpose for which it was processed). Additionally, Clause 19 limits the purpose of data portability which is incredibly important for mitigating harms by big tech. This is through the insertion of vague language in Clause 19(2) of the Draft Data Protection Bill, 2021 as a result of which, requests for data portability may be refused by Data Fiduciaries due to technical infeasibility. Further, such refusal will be specified in future by regulations. Clause 21 (2) also allows data fiduciaries to charge a fee for the exercise of rights by users. In the light of the above-mentioned exceptions to consensual processing of data, and weak user rights, we note that subscribers cannot exercise enhanced control over their data until these issues are resolved and user rights are strengthened, as well as exceptions narrowed. Here, the authority may submit it's view to the Ministry for Electronics and Information Technology specifically on concerns which emerge from a conflict from within it's approach when contrasted against the Data Protection Bill, 2021.

4. We also find the reliance on the technical architecture as proposed within the consultation paper that contains an infographic from "iSPIRIT Developers" to be troubling. The infographic is contained above paragraph 5.39 of the Consultation Paper below aims to facilitate the sharing of telecom data with other service providers ("insurance" "flow based credit"). This form of data aggregation will pose certain risk without an enforceable data protection law or authority to monitor and provide legal remedies. We caution against the adoption of this framework.

Question 48: 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?

Answer summary: *Consent is the bedrock of any data protection regulation. Here the DEPA framework is not anchored under a legal framework providing enforceable rights and remedies*

to end users. Further, DEPA also has technical limitations. 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 that are absent under DEPA. We suggest caution for adoption of DEPA or the consent stack for telecom subscriber or KYC data

1. The consultation paper argues that "*going to each TSP individually to access or share data becomes a lengthy and tedious exercise*" and that "*there is a lack of harmonisation around the regulations for data sharing within and across sectors*". In order to remedy these problems, the paper proposes the use of the consent manager framework as discussed in the draft Data Empowerment and Protection Architecture (DEPA) paper.[23] Under the DEPA framework Telecom Information Providers (such as Mobile companies, Internet Providers etc.) will be able to share user data with Telecom Information users (such as Banks, NBFCs etc.) after obtaining the consent of the users through consent managers. This is similar to the Account Aggergator framework which has been created by the RBI.[24] However, the paper does not specify the parties with whom telecom data can be shared. In case of AAs, the RBI, as per direction 3(iv) of the Master Direction-Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016, has the power to specify Financial Information Users with whom Financial Information can be shared.[25] This is less than ideal, as users do not have the ability of instructing the AA to share or not to share their data with a particular FIU.[26] The telecom data sharing framework laid out in the paper neither specifies the parties with whom telecom data can be shared nor does it refer to a regulatory authority which will have the power to specify 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.

---

[23] NITI Aayog; *Data Empowerment And Protection Architecture: Draft for Discussion;* Aug, 2020; https://www.niti.gov.in/sites/default/files/2020-09/DEPA-Book.pdf.

[24] *Explained: RBI's Account Aggregator Framework;* Internet Freedom Foundation; 28th Oct, 2021; https://internetfreedom.in/explainer-account-aggregator-framework-saveourprivacy/.

[25] Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016; 2nd Sept, 2016; https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598.

[26] Raghavan & Singh; *Regulation of information flows as Central Bank functions? Implications from the treatment of Account Aggregators by the Reserve Bank of India;* Paper for the 2020 Central Bank of the Future Conference Future of Finance Initiative, Dvara Research; Sept 2020; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3924793.

2. With DEPA, additional issues arise with respect to privacy and security. As we have noted before, given the unequal power relationship that may develop as a result of the dependence of consent managers on data users, consent managers may be incentivised to override the privacy and agency of users. Additionally, self-regulation may promote the use of lax standards of security which, for the scale at which DEPA is envisioned to be employed, would imperil the data of millions of citizens. For these reasons, it is necessary for public and statutory oversight to be present. To this end, it is welcomed that the framework envisions a prominent role for the Data Protection Authority proposed by the Personal Data Protection Bill, 2019. Additionally, the role of the Authority should not be limited just to imposing standards - it must take a proactive role in enforcement and monitoring.

3. The framework must through law lay down explicit safeguards for ensuring that consent managers comply with the principle of informed consent. This may be done by recommending a standard framework for consent sharing by a future Data Protection Authority. Moreover, opt-out models for consent sharing (where consent is presumed unless users opt-out) should be explicitly forbidden, especially for key sectors such as health and banking. We find such a recommendation to be extremely dangerous that will give rise to perverse incentives of, “consent hoarding”. It will shift the focus of business and technical models from recognising the autonomy of users towards obtaining meaningful consent (that will come with friction) towards achieving consent on scale by “tick-boxing” certain regulatory thresholds. This will be counter-productive to the aims of the present policy that focuses on user autonomy and consent.

4. Thus, we ask that the framework’s consent sharing standards adhere to the norms laid down by the GDPR in Articles 6, 7, 8, 9, 22, and 49. These rights need to be statutorily placed with the Draft Data Protection Bill and enforced by a Data Protection Authority. For granular and nuanced rules and regulations, the proposed Data Protection Authority may in future hold consultations with governmental bodies, industry bodies, and civil society to frame consent sharing mechanisms that are both growth-oriented and respect digital rights.

Question 49: Are there any other issues related to data ethics that require policy/regulatory intervention apart from the issues that have already been dealt with, in TRAI’s recommendations on the issue of ‘Privacy, Security and ownership of the Data in the Telecom Sector’ dated 16th July 2018 and the draft PDP Bill? Provide full details.

Answer summary*: We are troubled by the framing of the consultation paper which states, “till such time a general data protection law is notified by the Government, the existing Rules/Licence conditions applicable to TSPs for protection of users’ privacy be made applicable*

to all the entities in the digital ecosystem". This is another form of OTT licensing and beyond the regulatory ambit of the authority. 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. As a matter of statutory reading, the authority 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.[27] 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 Unified Access Service Licence. We further call for reform on the prohibition of use of bulk encryption as is presently contained in Clause 37.1 of the UAS licence.[28] The extension of such licence conditions to, "other stakeholders in the digital ecosystem" may further be counterproductive and undermine data protection and privacy of users.

3. We urge the TRAI to 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 on the foundation of privacy being a fundamental right of all Indian citizens flowing from the constitutional judgments of the Supreme Court of India.

Question 50: Stakeholders may also provide comments with detailed justifications on other relevant issues, if any.

---

[27] The Telecom Regulatory Authority of India Act, 1997, Telecom Regulatory Authority of India; https://trai.gov.in/sites/default/files/The_TRAI_Act_1997.pdf

[28] Licence Agreement For Provision Of Unified Access Services, Department Of Telecommunications; https://dot.gov.in/sites/default/files/UAS%20license-agreement-19-12-2007.pdf?download=1

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 the absence of any reform of surveillance powers. Given large amounts of personal data are transmitted through smartphones, in addition to the existing regulations, a comprehensive legislation needs to be made following the principles of the nine-judge bench judgement on the right to privacy. Here the authority may examine the feasibility of study and a consultation on the opaque, antiquated and deficient regulatory system of surveillance that is principally applicable to TSPS.*

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 P*eople'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 led 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 the existence of mass surveillance. This not only conflicts with the 1996 PUCL judgement 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.

3. The proposed Data Protection Bill, 2021 does not contain any provisions for surveillance reform. 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 safeguards to protect the privacy of citizens.