Counter-Comments to TRAI for the Consultation Paper on the Regulatory Framework for Promoting Data Economy

We thank the Telecom Regulatory Authority of India ('TRAI') for inviting comments on its Consultation Paper on a Regulatory Framework for Promoting Data Economy Through Establishment of Data Centres, Content Delivery Networks and Interconnect Exchanges in India[1] (the 'Paper'). TRAI received comments on the Paper until 10th February 2022, and published comments by stakeholders. We at Indian Software Product Industry Roundtable ('iSPIRT') would like to share counter-comments in relation to Questions 47-50 of the Paper, i.e., Chapter 5 on 'Data Ethics- Privacy, Ownership and Security'. We would specifically like to discuss the issue of bringing telecom data onto the current Account Aggregator framework.

1. Introduction

1.1 Relevant recommendations under Chapter 5:

Chapter 5 makes several suggestions on the privacy of telecom users, including the development of a data sharing and consent management framework for the telecom sector similar to Ministry of Electronics & Information Technology ('MeitY's') Electronic Consent Framework[2] and the Account Aggregator ('AA') framework[3]. These recommendations were also made earlier in 2018[4]. The Paper highlights important issues like the challenges with sharing telecom subscriber data like different data formats, sharing of physical documents, protecting from misuse, etc. It also highlights the position of the individual, in terms of the asymmetry between himself and the custodians of his data, misuse via marketing, lack of rights to access, view or amend his own data, etc. Discussing solutions, the Paper suggests adopting Data Empowerment and Protection Architecture ('DEPA')[5] in the telecom sector,

---

[1] TRAI Press Release: *TRAI releases Consultation Paper on 'Regulatory Framework for Promoting Data Economy Through Establishment of Data Centers, Content Delivery Networks, and Interconnect Exchanges in India'*, Press Release No. 58 / 2021, Consultation Paper No.10/2021, accessible at https://www.trai.gov.in/sites/default/files/CP_16122021_0.pdf
[2] MeitY Notification: Electronic Consent Framework: Technology Specifications, available at https://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf
[3] RBI Notification: *Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016*, RBI/DNBR/2016-17/46, dated September 02, 2016, updated October 05, 2021, accessible at https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10598
[4] TRAI Press Release: *TRAI releases Recommendations on "Privacy, Security and Ownership of Data in the Telecom Sector"*, Press Release No.78/2018, dated July 16, 2018, accessible at https://www.trai.gov.in/sites/default/files/PRNo7816072018.pdf
[5] Niti Aayog Press Release: *Data Empowerment and Protection Architecture: A Secure Consent-Based Data Sharing Framework to Accelerate Financial Inclusion*, dated August 20, 2020, accessible at https://www.niti.gov.in/sites/default/files/2020-09/DEPA-Book.pdf

allowing Telecom Service Providers ('TSPs') to become Financial Information Providers ('FIPs'), to enable subscribers to access their data and share it with third party-institutions. Finally, the Chapter ends with a note that it is important to create such an electronic framework for better management of user consent.

1.2   Comments in response:

Comments in response to Chapter 5 are varied. While appreciating the potential of unlocking telecom data for the social and economic betterment of individuals, stakeholders have also raised some concerns. Some of these are highlighted below:

- Difficulties in implementing DEPA in the telecom sector due to non-uniform applicability of privacy regulations across sectors
- A need to delay until the (Personal) Data Protection Bill, 2021 (PDP Bill')[6] is made into law due to possible conflict/duplication of law or for better protection of data principals
- A requirement to further study and learn from the current AA framework prior to implementation
- A difference in the stringency of applicable privacy/ security obligations as applicable to TSPs vs. potential users of the telecom data raising privacy concerns

1.3   iSPIRT's counter-comments in brief:

To these comments, we would like to suggest that apart from considering the development of a new, equivalent system to DEPA and AA for the telecom sector, it is also worth exploring bringing telecom data into the AA framework itself, in its current form, in more detail. As per the Niti Aayog paper on DEPA[7], on 28 August, 2020, TRAI had announced a TRAI-RBI partnership at a 'Telecom Subscriber Empowerment' workshop, which would allow telecom companies to become FIPs in the AA system. This should be taken forward.

A significant advantage this brings from a consumer perspective is that this allows a single cross-sectoral consent manager, compared to a multiplicity of consent managers (i.e., AAs for the financial sector, separate consent managers for the telecom sector, etc.). Financial inclusion for example is a crucial use-case for telecom data. Here, to be able to use a single consent manager to access and share the required data, be it financial data or telecom data, with the same Financial Information Users ('FIUs') and for similar purposes (like credit or insurance access), will reduce the burden for the consumer. This applies from the perspective of sharing and managing consent, exercising rights under the framework, etc. for the customer. The same benefits can also accrue with other important use-cases with telecom data like fraud prevention. DEPA as a framework can accommodate and enable such cross-sectoral data sharing.

This way, TSPs could be directly onboard as FIPs in the current AA framework, allowing users to provide consent-based access to their data being held with the TSPs to the FIUs. Apart from these general benefits, to specifically address some of the comments in response to the Paper (listed in Section 1.2

---

[6] Lok Sabha Secretariat Notification: *Report of the Joint Committee on the Personal Data Protection Bill, 2019*, dated December 16, 2021
[7] Supra Note 5.

above), privacy risks with bringing telecom data onto the existing AA framework need to be viewed and evaluated differently from creating a new AA framework altogether for the telecom sector. For example, given the current restrictions of the AA framework, only regulated entities in the financial sector can gain access to data, and user consent is essential for data to be shared. The AA framework itself has multiple privacy safeguard, such as the AA being data blind, sharing of data in encrypted form only, etc. Further, similar to TSPs, current FIUs being regulated entities only are also subject to separate Reserve Bank of India ('RBI') and other norms to maintain customer confidentiality and privacy, and for consent based data sharing with third parties[8].

We would like to submit that the possibility of onboarding TSPs onto the AA framework merits further exploration. A second round of consultation inviting stakeholder views specifically on the feasibility, advantages and risks of such an integration would thus be welcome.

2. <u>Some advantages of bringing telecom data onto the current AA framework</u>

The Paper already touches upon the merits of such a step. These and some additional points are summarised below:

2.1 Utilising telecom data for financial inclusion:

Para 5.36 of the Paper highlighted that telecom data is often the first digital footprint generated by a low-income household, and a steady history of on-time recharges could contribute to building a credit history. This is an important point in favour of bringing telecom data onto the current AA framework.

For those citizens at the bottom of the pyramid with a lack of financial history, access to capital for self-improvement and growth through the formal financial system players such as banks is either non-existent or usurious/ costly. For example, a vegetable vendor who makes purchases in the wholesale market in the morning and sells in the retail market during the day, with all transactions happening in cash, leaves no data or transaction footprint, making it impossible to provide funding through the organised financial system. If such a vegetable seller's data, like his prepaid phone recharge history, were to be made available to a specialised financial institution, it may be able to extend credit for working capital on a daily basis easily or a loan for putting up a new stall over time.

Here, consumers can be considered "credit invisible" if they either (1) do not have any credit history with Credit Information Companies ('CICs') or (2) if their histories are too scant or old ("thin") to generate a credit score. According to estimates, ~550-600 million 'banked' population do not have a credit history and another ~300-400 million are not scoreable (unbanked). As on December 2021, telecom penetration is ~1.2 bn against a population of ~1.3 billion, of which Urban: ~655.2 million and Rural: ~523.2 million.

---

[8] RBI Master Circular: *Master Circular on Customer Service in Banks*, RBI/2015-16/59, dated July 1, 2015, accessible at https://www.rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=9862; RBI Circular: *Directions on Managing Risks and Code of Conduct in Outsourcing of Financial Services by NBFCs*, RBI/2017-18/87, dated November 09, 2017, accessible at https://rbi.org.in/scripts/BS_CircularIndexDisplay.aspx?Id=11160; RBI Master Directions: *Master Direction on Digital Payment Security Controls*, RBI/2020-21/74, dated February 18, 2021, accessible at https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD7493544C24B5FC47D0AB12798C61CDB56F.PDF

With almost ~1.2 bn population generating telecom transaction data on almost daily basis mirroring attributes like (i) purchasing power / affluency (handset type, Average Revenue Per User ('ARPU'), recharge/bill plan amount), (ii) ability to pay (recharge / bill plan payment history), financial inclusion could be significantly enhanced. For example, credit worthiness can generally be proxied by usage (ARPU), age on network, device type and type of connection (prepaid or postpaid).

Porting of telecom data can open the gates for financial inclusion to the 600-700 million "invisible" population a large part of which may be credit worthy potentially.

2.2   Bringing SMEs into the formal financial system

Similarly, for small businesses, which are the most excluded, this can be a game changer for access. For example, the reach and scale of 'mom and pop' retailers drive 90% of the telco's recharge revenue and more than 98% of new acquisitions. These small and medium enterprises (~1 Mn across all states) are usually 100% cash driven business with limited or ZERO digital footprint and can be provided credit, insurance etc. and brought into formal financial system.

2.3   Repurposing telecom bills from KYC uses alone

TSPs already provide subscribers access to their own data via physical records as monthly bills or through digital portals which the subscriber is free to share with anyone like a bank for receiving financial services. Telecom bills have long been accepted for KYC (address proof) and other such services. TRAI has been issuing consultation papers and guidelines for providing bills to subscribers over the years which harmonises the billing process of different TSPs, whether in hard copy, soft copy or access on TSP's portal or through mobile app. TSPs maintain extensive data with respect to a subscriber's overall activity that is used for creating the bill as represented by Call Data Records (CDR'). Some of this billing data and CDR can also be made available to be shared with consent of the subscriber under the AA framework for receiving services.

2.4   Advantages to TSPs

Broadly, this creates potential for a TSP to take on 3 roles- of a data provider, a data user, or even a consent manager. Providing access both ways can also be considered, so along with providing telecom data as FIPs the TSPs would be able to access financial data for their customers through the AA framework as FIUs. This would enable them to provide better services for their customers such as increasing their credit limit or providing an option to switch from prepaid to postpaid services. In such a new paradigm, compensation to TSPs can happen in a number of ways:

- First, they would get reciprocal access to financial information on their customers, as FIUs to enhance their core business and build on their role.
- Second, they can choose to levy a small fee for sharing the data with AAs in accordance with market pricing as it evolves, without charging anything additional to their subscribers.

- They could also eventually capitalise on the new opportunities presented by this model to build a new business as intermediaries to provide services related to credit, wealth management, insurance etc, as LSPs.
- In addition, TSPs could act as Consent Managers or AAs* for their subscribers through an appropriate structure, such as a subsidiary, where they could compete with other AAs by providing a better user experience ('UX') as a Consent Manager and provide other value added services.

2.5   Others

There are other use cases, such as preventing fraud in the system, that affect users at all levels. For instance, in relation to identity and fraud management, the following use-cases are possible:

- **Identity as a Service:** TSPs can offer linking of device, sim and location to provide seamless authentication services. They can also offer alternative, OTP-free two-factor authentication via API (alternative to Ashield/ RouteMobile).
- **Prove identity theft:** Additionally, factors like location data and identified 'normal patterns' can help establish identity theft or even links to risky profiles. Anomalies like sim swaps and change of device handsets can be flagged.
- **Reduce card fraud:** They can also help reduce card fraud via location or card present transactions or chargeback history for card not present transactions via SMS A2P.

3.   The Account Aggregator framework as utilized by the TSPs:

To enable data flows via an AA under the current framework, the TSP would need to:

- implement interfaces that will allow an AA to submit consent artefacts, and authenticate each other, and would enable secure flow of telecom information to the AA;
- adopt means to verify the consent including digital signatures, if any, contained in the consent artefact;
- implement means to digitally sign the telecom information that is shared by them about the customers;
- maintain a log of all information sharing requests and the actions performed by them pursuant to such requests, and submit the same to the AA.
- Ensure that the user is able to use or avail of the services offered without being coerced into providing the personal data.

4.   Concerns to be addressed

Bringing telecom data onto the AA framework in its current form will also raise concerns with privacy and inter-sectoral data exchange, as highlighted in the Paper. Without going into these concerns in detail, a few points which can be considered to mitigate this risk include:

- **Identify the categories of telecom data to be shared:** There are multiple categories of data that TSPs possess, of these the categories that can be shared via the AA framework should be identified, for eg. KYC data, Billing History, Call Data History (with all third party personal data either anonymised/redacted), dynamic Location data in aggregate terms such as general location in day and at night etc, or estimated parameters such as variability of location etc. It is to be noted that two of the three data types are already available for the user in the form of itemised mobile bill as per various TRAI rules and the third category is proposed only in query form for confirmation to minimise fraud only. No location based services that builds hyper local services to be presented to user based on location are proposed to be allowed in this exercise.

- **Exclude OTT related data:** Also, only data that a TSP has in its capacity as a TSP be considered for sharing, data it has in its capacity as an over-the-top ('OTT') service provider (in-house apps, etc.) should be excluded.

- **TRAI as the regulatory representative in the AA framework:** Currently, the AA framework is regulated by the RBI as a representative regulator under Financial Stability and Development Council ('FSDC') which has SEBI, IRDAI etc., with Dept. of Revenue being added as a proxy for GST data sharing. It is proposed that TRAI becomes a representative of Telecom sector to enable this cross sector data sharing which will help
  - Technical aspects such as standards to be defined
  - Leverage role of ReBIT in the AA framework, to bring together various industry participants, bringing technical standards and documentation and hosting sandbox for testing
  - Enable development of Technical Standards Organisations ('TSOs') and Self-Regulatory Organisations ('SROs')

We hope our comments will be taken into consideration and look forward to next steps. In case any further information or clarifications are needed, please feel free to contact us.

About iSPIRT Foundation

iSPIRT Foundation is a nonprofit technology think tank based in Bangalore composed of public spirited volunteers who have contributed to many national digital platforms including eKYC, eSign, UPI, DigiLocker, ABHM, UHI, FASTag, Bharat Bill Payments System, RBI Account Aggregator, etc. iSPIRT has submitted the recommendations outlined below in the spirit of civic contribution. iSPIRT or its volunteers do not gain financially in any way from adoption of these recommendations. For more visit www.ispirt.in or email us at community@ispirt.in