November 21, 2017

To,

1. Shri R.S. Sharma
   Chairman
   Telecom Regulatory Authority of India (TRAI)
   New Delhi

2. Shri Arvind Kumar
   Advisor (Broadband and Policy Analysis)
   Telecom Regulatory Authority of India (TRAI)
   New Delhi

3. Shri Bharat Gupta
   Joint Advisor
   Telecom Regulatory Authority of India (TRAI)
   New Delhi

Re: Additional Comments in Response to TRAI Consultation on Privacy, Security and Ownership of Data in the Telecom Sector

About us

Koan Advisory Group is a New Delhi based policy advisory firm, which combines thorough domain knowledge across multiple technology oriented sectors with continuous engagement of decision makers in industry and government. We have previously engaged with various regulatory arms, including TRAI on issues related to telecommunications and future policy making.

Submission

We laud this initiative of the TRAI to onboard public comments to inform its recommendations regarding India's revised data protection framework. As highlighted in our submission, the current technological landscape is heavily based on information flows taking place in real time. This entails a constant flow of across sectors, across borders and across networks and devices. In this backdrop, it is important for data protection frameworks to incorporate policy and legal provisions that promote innovation based on trust within the ecosystem. In such light, it is imperative that India embrace a regime which enables a robust and secure information sharing landscape, and leverage this to underpin its position as a serious contender in the global marketplace for innovation. Thus, a forward-looking policy requires data privacy be recognised as the principal differentiator driving development of products and services in India.

Against this background, these are some additional comments Koan Advisory Group wishes to offer with respect to the risk based framework proposed in our submission. The earlier submission can be accessed here.

Risk Based Approach to Data Protection

With the emergence of new categories of data, a one-size-fits-all approach cannot adequately address information security and privacy challenges. Thus, organisations need to account for factors such as the type of data, the size of the data processing operation, the intended purposes of the processing and uses of the data, the number of envisaged data transfers, as well as the privacy risks to individuals. A risk based approach to data protection can help organisations effectively account for these factors. The OECD has identified that operationalising a risk based approach will broadly entail the following elements:

1. Accountability, which entails giving effect to policies and obligations through appropriate mechanisms and procedures, and being answerable to regulators and stakeholders for compliance.
2. Risk assessment, based on credible information, which is reflective of the interests of stakeholders, and which takes human and cultural factors into account.
3. Enforcement through privacy regulation that penalises significant and predictable harms through sanctions that can create financial, legal and reputational risks, and alternative mechanisms such as certification and Binding Corporate Rules.

Such a risk based framework for data privacy further addresses the shortcomings of models that rely on user consent, which is often meaningless considering the common lack of understanding of the true import of sharing their data amongst users.

A further policy recommendation in this light is the operationalisation of a cyber risk insurance framework, which engages insurance mechanisms to effectively evaluate risks, which can then be leveraged by organisations in operationalisation their data protection policies. A recently concluded project by the OECD on "*Enhancing the Role of Insurance in Cyber Risk Management*" has highlighted that legal frameworks for data protection are important drivers of compliance costs, which include fines and penalties, incidence response costs, reputational damage and privacy breach compensations.

In India, cyber risk insurance models are emerging with several insurance companies designing and managing new insurance products geared specifically towards cyber risks. However, institutions have reportedly been slow to take up such policies owing to a lack of understanding of cyber risks and costs. Furthermore, it has been identified under the OECD project report that insurance products for cyber risk require the availability of incident reporting data, threat analysis and risk management expertise necessary to reduce uncertainty about cyber risk exposure and too facilitate the development of probabilistic pricing and exposure management models of assessing risk. In this light, it is recommended that information sharing regarding privacy breaches be incentivised through appropriate policies at the national level. Further, it is recommended that the government examine the role of regulatory authorities in contributing to data availability and the existence of impediments to data sharing.

Cross Border Data Flows and Data Localisation

Cross border jurisdiction issues highlight the necessity of appropriate responses regarding cross border data transfers. As already mandated under the extant data protection regime in India, entities can only transfer data across jurisdictions where an equivalent level of data protection is adhered to. At the same time, several distinct approaches to manage such information flows exist globally, which

range from consent-based cross border data transfers to data localization requirements. Particularly, several stakeholders to the consultation have called for local hosting requirements.

It must be noted that these are generally restricted to specific sector information, and remain less commonly adopted for generic data. In this light, it is recommended that data localization requirements be restricted to specified types of data. Furthermore, data localization requirements should allow for transfers and storage of data in other jurisdictions that offer an equivalent level of data protection. This facilitates data redundancy which is a recognised best practice for ensuring security of data by enabling recovery of information assets in case of a cyber security event. Thus, specific other approaches to managing cross border data flows such as mutual acceptance agreements, adequacy shields, along with binding corporate rules and model contracts should be evaluated critically for their strengths and limitations. The new data protection framework for India must consider each of these approaches and evaluate them for the trade-offs each of these entail to address cross border challenges to data sharing whilst also enabling necessary data flows.

In addition to the above, we wish to make the following additional comments:

- It is important further to consider instances wherein device manufacturers have allowed backdoors into devices that allow unauthorised access to user information such as IMEI numbers, mobile network names, serial names, as well as user behaviour information. Notably, these backdoors existed without user knowledge or consent. Such instances underpin the importance of data protection policies that require mandatory opt-in requirements for users especially where user data that is inessential to the provision of services is being collected.

- While a number of responses have highlighted the primacy of informed consent, mechanisms for obtaining consent need to be reviewed in light of the new ways in which users interact with data based businesses. Under the extant data protection provisions under the Information Technology Act and Rules, user consent is a blanket requirement for the collection of sensitive personal data or information. As noted by several other responses, such requirements need to be further nuanced as per the context of data processing and the nature of data being collected. At the same time, policymakers must remain mindful of the information asymmetries that exist among users in India. Informed consent principally requires that consumers are aware of the implications that data sharing entails. Thus, digital literacy should be a principal focus of data protection policies, particularly given that India's own digital literacy missions have been inadequate. Here, the private sector service providers which actively interact with users should be co-opted to drive digital literacy programmes. For instance, large internet companies are currently investing millions of dollars in digital literacy programs that are meant to teach internet literacy to new users and digital job skills to the unemployed across jurisdictions, ranging from the United States of America to Nigeria.

- Several stakeholders have referred to the proprietary nature of datasets in the context of information sharing. Such comments need to be evaluated further to assess the true nature of anonymised datasets. In this context, it is important to differentiate between raw data as opposed to aggregated sets of data and the intellectual property rights that accrue for each of these categories, along with the fair use exceptions that apply.