Issues for Consultation:

Question 1: Are the data protection requirements currently applicable to all the players in the eco-system in India sufficient to protect the interests of telecom subscribers? What are the additional measures, if any that need to be considered in this regard?

Redmorph Recommendation:

The laws on personal data are ambiguous. Indians are repeatedly transmitting their personal information for various activities due to low awareness –firstly that they are actually sharing data and secondly that it can be misused. Personal data should be collected for legitimate purposes and be used for the purpose it has been specified. The landmark ruling on 24th August, 2017 decided that privacy is a fundamental right and called upon the government to examine and put in place a robust regime for data protection.

Measures to be considered:
Privacy policies or data consent by operators/apps or other stake holders needs to be within a particular word limit. (Currently Apple's privacy policy for India reads over 3000 words and Microsoft's over 7000 words- majority of the users wouldn't read this.) Language used should be simple and understandable.

Since India is in an early stage for developing the legislature on privacy, there is an opportunity to be relevant to the digital age and keeping in mind the widespread Internet of Things (IoT). The legislative path allows India to develop world-leading data protection that moves away from the flawed notice-and-choice model to one that establishes for the government and private sector alike clear, predictable parameters on the collection, use, processing, sharing, and the security of personally identifiable information. The Supreme Court's recognition of a right to privacy provides the foundation to ensure that innovations such as Aadhaar are used to enhance the poor's dignity, well-being, and security, and not for opportunism for private service providers and data brokers.

Question 2: In the light of recent advances in technology, what changes, if any, are recommended to the definition of personal data? Should the user's consent be taken before sharing his/her personal data for commercial purposes? What are the measures that should be considered in order to empower users to own and take control of his/her personal data? In particular, what are the new capabilities that must be granted to consumers over the use of their personal data?

Redmorph Recommendation:

It is important to understand the ability of an app or data collector to collect data and the purpose for which it is collected. Once data is collected, there are 3 broad categories how this may be used:

1) The app or data collector uses the data only for the purpose it has been asked for and does not allow any 3rd party access to this.
2) The app or data collector gives access to user data to other 3rd parties.
3) The app or data collector gives access to other 3rd parties to collect user data.

For points 2 and 3 (access to data to 3rd parties and giving access to 3rd parties to collect user data directly) there needs to be a set of rules in place. App permissions obtained by the app owner should not necessarily transfer to the 3rd parties and the 3rd parties should ask for these permissions directly from the user.

This brings us to define collection of personal data elaborately. Keeping in mind the current advances in technology, there should be a compliance policy that checks the principles of personal data and relates it to the usage mentioned above. Without an audit by a centralized privacy committee, the app or data collector can be deemed unlawful.

A comprehensive report published by the Center for Internet and Society (cis-india.org) articulates the principles and process of Personal data collection:

1) **Notice:** A data controller shall give simple to understand notice of its information practices to all individuals, in clear and concise language, before any personal information is collected from them.
2) **Choice and Consent:** A data controller shall give individuals choices (opt-in/opt-out) with regard to providing their personal information, and take individual consent only after providing notice of its information practices. Only after consent has been taken will the data controller collect, process, use, or disclose such information to third parties, except in the case of authorized agencies. The default setting should be opt-out and data collection should happen only after user has explicitly given their consent.
3) **Collection Limitation:** A data controller shall only collect personal information from data subjects as is necessary for the purposes identified for such collection, regarding which notice has been provided and consent of the individual taken. Such collection shall be through lawful and fair means.

4) **Purpose Limitation:** Personal data collected and processed by data controllers should be adequate and relevant to the purposes for which they are processed. A data controller shall collect, process, disclose, make available, or otherwise use personal information only for the purposes as stated in the notice after taking consent of individuals. If there is a change of purpose, this must be notified to the individual.

5) Access and Correction: Individuals shall have access to personal information about them held by a data controller; shall be able to seek correction, amendments, or deletion such information; be able to confirm that a data controller holds or is processing information about them; be able to obtain from the data controller a copy of the personal data.

6) **Disclosure of Information:** A data controller shall only disclose personal information to third parties after providing notice and seeking informed consent from the individual for such disclosure.

7) **Security:** A data controller shall secure personal information that they have either collected or have in their custody, by reasonable security safeguards against loss, unauthorised access, destruction, use, processing, storage, modification, de-anonymization, unauthorized disclosure [either accidental or incidental] or other reasonably foreseeable risks.

8) **Openness:** A data controller shall take all necessary steps to implement practices, procedures, policies and systems in a manner proportional to the scale, scope, and sensitivity to the data they collect, in order to ensure compliance with the privacy principles, information regarding which shall be made in an intelligible form, using clear and plain language, available to all individuals.

9) **Accountability:** The data controller shall be accountable for complying with measures which give effect to the privacy principles. Such measures should include mechanisms to implement privacy policies; including tools, training, and education; external and internal audits, and requiring organizations or overseeing bodies extend all necessary support to the Privacy Commissioner and comply with the specific and general orders of the Privacy Commissioner.

Based on the above principles, we suggest that an individual has the following tools to ensure their privacy. This should be at a practical device level. It should protect an individual from invasion of privacy at a telecom, device and app/content level. These would be:

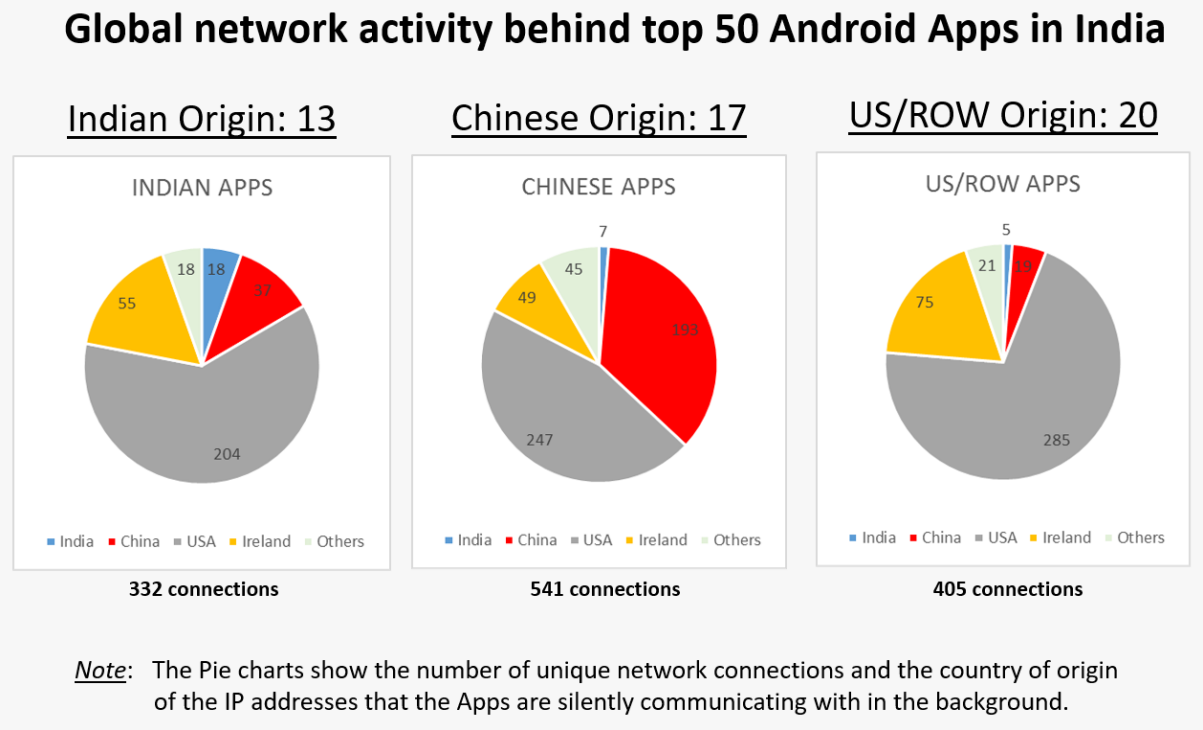
1. VPN or Encrypted proxy
2. Device firewalls
3. Tracker blockers
4. App permission managers

Question 4: Given the fears related to abuse of this data, is it advisable to create a technology enabled architecture to audit the use of personal data and associated content? Will an audit based mechanism provide sufficient visibility for the government or its authorized authority to prevent harm? Can the industry create a sufficiently capable workforce of auditors who can take on these responsibilities?

Redmorph Recommendation:

Yes, technology enabled architecture can help misuse of personal data. However, it should be used at a data/content usage level and also at an audit level. Every app sold in India (free or paid) on Google Play Store, iTunes, etc. should openly declare the network connections made and their country of location, ownership entity, purpose & data collection.

We analyzed the top 50 Android apps used in India according to the analytics firm App Annie and Google PlayStore. The charts below summarize the internet connections made by each App and the location of these IP addresses:



- The top 50 Apps were created by companies in 10 different countries.
- These 50 Apps together were communicating with over 1278 unique domains/IP addresses in over 10+ countries.
- The number of unique IP addresses that an App connected with in the background varied quite a bit and ranged from 2 to 76. (Note: this number can vary for the same app from time to time.)

- Over 99% of the network connections on average were communicating with IP addresses or servers outside India.
- Even Apps produced by Indian companies had over 95% of their connections with IP addresses or servers outside India.

Our investigation showed that these domains and IP addresses belonged to several companies. In addition to connecting with IP addresses belonging to the App producer, the Apps were mostly connecting with entities such as Ad networks, Social Media networks, Data brokers, App/Site Analytics, Audio/Video content providers, CDN, etc. There were several IP address or domains we could not identify their purpose or who they were.

Question 8: What are the measures that should be considered in order to strengthen and preserve the safety and security of telecommunications infrastructure and the digital ecosystem as a whole?

Redmorph Recommendation:

Telecom providers have not only detailed profile info of the users especially now with Aadhar based validation but also usage information. Basis the user information and strong analytical capabilities that the telcos have developed over the years, telcos have large amounts of data. This data is personal and hence its privacy is of utmost importance.

While telcos tend to have strong data security and privacy norms they work with outsourced service providers like call centres, collection agencies etc. who are susceptible to data leaks. TRAI needs to have a min policy framework set for data privacy.

Telecom operators are working to monetize the user data for mobile marketing. Care needs to be taken that personal information cannot be shared with marketing organizations without proper compliance as mentioned in the above points.