Annexure A

Idea Cellular response to TRAI Consultation paper on Privacy, Security and Ownership of Data

PREAMBLE

As rightly pointed out in the Consultation Paper, the rapid evolution of telecommunications services in India has aided better connectivity among users and increasing use of information and communication technology (ICT) services. Parallely, the user's interaction with ICT services, whether through traditional telecom services, Internet services, devices, applications or other forms of content has led to a quantum leap in the quantity and type of data that is getting generated at each step of the interaction. It is thus critical that data protection and security are given utmost importance so that subscriber confidence towards the medium of Internet is not adversely affected and there is a large scale adoption of internet in keeping with the vision of the Hon'ble Prime Minister of India.

It has always been the prerogative of TSPs to maintain public trust and safety / security of customer data, and accordingly they have built up powerful systems to combat any threats arising on this account. Currently, the different requirements for data protection which telecom operators are bound to adhere to through the telecom regulatory framework are those emanating out of sector specific laws (Indian Telegraph Act 1885, Indian Telegraph Rules 1951), requirements as part of License agreement, various Guidelines and directives of the TRAI including National Customer Preference Register (NCPR), etc. Additionally, there are various conditions as well as general provisions contained in the Information Technology Act, 2000 that the TSPs need to be compliant to.

In our considered opinion, all these provisions are sufficient to protect the data that TSP's (Telecom Service Providers) have or carry in respect of the telecom subscribers, and there is no need for any additional mandates for the TSPs that already have a long history of success in this task, guaranteeing both the privacy of their users and the security of their networks.

Currently some of the services being provided by OTT players are a perfect substitute of Telephony services offered by Licensed Telecom Service Providers (TSPs) in India. However, while the licensed network operators are long-term contributors to Indian economy, and are faced with continuing demands for investments to improve their services (in particular, to install broadband, increase network capacity and network quality), the OTT players offering comparable services operate in a completely free, 'unregulated' market environment. There are various compliances that are followed by the TSPs but not by the OTTs offering communication services.

We believe that to fully protect the interests of telecom subscribers, all entities in the ecosystem that deal with personal or sensitive data should be regulated by strong privacy and security laws, and such laws should be equally and uniformly applicable to all the players in the digital eco-system.

Towards that end, there is a need for an overarching framework/legislation that addresses comprehensively the definition of Personal Data and its protection mechanism, and reaches out beyond the TSP's to include all organizations and entities in the digital ecosystem that are involved in collection, processing and usage of personal data.

Lastly, it is important that while considering the definition of personal data, no distinction is made out in respect of the source of data, whether user provided or system generated – the principles of data privacy should apply to all data that qualifies to be "personal Information" by nature. However, for data that is "Anonymized or Aggregated" in nature, and cannot be used to identify a person directly or indirectly, i.e., it is not "Personal information" or "Personally Identifiable information" by nature, there should not be a requirement for any "User Consent". Declarations in respect of such information can be a part of the Organizations' Privacy Policy where disclosures on what personal information is being collected; purpose for collection and its use; whether it will be disclosed to third parties; notification in case of data breach, etc. can be duly mentioned.

.

Our Query wise response is as under:

Q1. 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?

Idea Submission:

- As mentioned in the Consultation Document, Data Protection may be broadly defined as the legal control over access to and use of data stored in the digital format. It may also be considered as a process of safeguarding digital information from corruption and/or loss.

- The different requirements for data protection which telecom operators are bound to adhere to through the telecom regulatory framework are those emanating out of sector specific laws (Indian Telegraph Act 1885, Indian Telegraph Rules 1951), requirements as part of License agreement, various Guidelines and directives of the TRAI including National Customer Preference Register (NCPR), etc. Additionally, there are various conditions as well as general provisions contained in the Information Technology Act, 2000 that the TSPs need to be complaint to.

- **In our considered opinion, all these provisions are sufficient to protect the data that TSP's (Telecom Service Providers) have or carry in respect of the telecom subscribers, and there is no need for any additional mandates for the TSPs that already have a long history of success in this task, guaranteeing both the privacy of their users and the security of their networks.**

- **Currently some of the services being provided by OTT players are a perfect substitute of Telephony services offered by Licensed Telecom Service Providers (TSPs) in India**. However, while **the** licensed network operators are long-term contributors to Indian economy, and are faced with continuing demands for investments to improve their services (in particular, to install broadband, increase network capacity and network quality), the OTT players offering comparable services **operate in a completely free, 'unregulated' market environment**. There are various laws such as those mentioned below that are followed by the TSPs but not by the OTTs offering communication services.

- **<u>Relevant telecom laws/regulations being followed by TSPs and not by OTTs</u>**

    1. **No Payment of Regulatory levies and License fee, other taxes.**

    2. **OTT players are not required to follow customer-centric regulations:**
        - Telecommunications Tariff.
        - Quality of Service norms
        - Metering and Billing norms
        - Complaint Redressal Mechanism:
        - Unsolicited Commercial communications (UCC)
        - Data privacy and Security.

    3. **National Security and other norms which OTT players do not follow.**
        - Telecom companies are to be registered in India
        - Domestic traffic to stay within India:
        - Network to be set up within service area or country: Lawful interception:
        - Usage of Higher Encryption Key
        - Access to subscriber database:
        - Maintenance of CDR/IPDR: ISP cannot connect with PSTN/PLMN.
        - Emergency services

- OTT Players that offer communication services are thus in violation of existing laws or matters of common public interest like privacy, national security etc. Similarly, there are many other players in the telecom and digital ecosystem (such as Third party data aggregators, telecom service resellers, device manufacturers, mobile OS manufacturers, mobile app creators, etc.) that deal with personal data and in many cases collect data that is equally or more sensitive than that which TSPs collect. For instance, job portals and mobile apps have sensitive personal data on an individual's address, employment history and compensation, etc. While TSPs are regulated and employ data protection measures, a limited mandate is applied on these other players in the digital ecosystem.

- **We believe that to fully protect the interests of telecom subscribers, all entities in the ecosystem that deal with personal or sensitive data should be regulated by strong privacy and security laws, and such laws should be equally and uniformly applicable to all the players in the digital eco-system**.

- **There is thus a need for an overarching framework/legislation that addresses comprehensively the definition of Personal Data and its protection mechanism, and reaches out beyond the TSP's to include all organizations and entities in the digital ecosystem that are involved in collection, processing and usage of personal data.**

Q2. In 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?

Idea Submission:

- As per current definition in the IT Act: "Personal information" means any information that relates to a natural person, which can be used, either directly or indirectly for identifying such a person."

- "Sensitive personal data or information" is defined to be a sub-category of this information, to include items such as passwords, financial information, health conditions, sexual orientation, etc.

- **Idea Cellular believes that even in light of technological advances, the definition of personal data as mentioned above is sufficient and may be continued with.**

- **However, we feel that the definitions of sources, as related to personal data would need to be addressed in view of the recent advances in technology**.

Sources:

i. In light of recent advances in technology, newer sources of personal data should be considered. While traditionally the source of personal data has been the "user" himself/herself (such as when the user submits forms, digital or physical, with personal data in them), now, personal data can be generated by data controllers and data processors as well. For instance, many mobile applications collect a wide variety of data such as handset information, times of usage, types of usage, location information. While each of these pieces of information on their own may not count as personal data, in combination they can be used to build an individual's profile.

ii. It is important that while considering the definition of personal data, no distinction is made out in respect of the source of data, whether user provided or system generated – the principles of data privacy should apply to all data that qualifies to be "personal Information" by nature. However, for data that is "Anonymized or Aggregated" in nature, and cannot be used to identify a person directly or indirectly, i.e., it is not "Personal information" or "Personally Identifiable information" by nature, there should not be a requirement for any "User Consent". Declarations in respect of such information can be a part of the Organizations' Privacy Policy where the intended use of such information and the categories of recipients can be mentioned.

- **<u>Measures for a User to take control of his data:</u>**

i. The following factors should be considered on this issue:
   a. Whether the data is personal or not (such as anonymized or aggregated)
   b. Whether data is being used for the purposes stated
   c. Implied consent v/s explicit consent
   d. Whether data is being used by entities for providing or improving their own services or for other purposes

ii. For all collection of data, which is personal in nature, proper notice should be provided to users by all entities performing such collection

iii. Entities may use personal data for providing their services as would be stated in their agreement with their customers. Additionally, entities may use the personal data to enhance/improve the

services or offerings made to their customers. For any other use of personal data, beyond this, explicit consent should be collected by the Data Controller. The consent should state:

a. The type of data / personal information that will be collected
b. The purpose for which it will be used
c. The consequence of data being used
d. The retention period for this data
e. The Data Processors, if any, that will be involved in the data being used, which will have access to this data

iv. The liability of collection and storage of user consent should lie on the Data Controller, or the entity directly interacting with users. This should include consent for sharing data with any Data Processors that are involved in the execution of the purpose

- **<u>New Capabilities granted to users:</u>**

i. It is critical that the users are provided with the option to opt out of the consent for sharing of personal data, as and when desired. This may require them to withdraw from the service being provided and/or wait for a certain processing period but the option has to be available to the user. Complete procedure for the same along with the details of timelines, consequences, etc. should be made easily available to the user.

ii. A mechanism for the users to view and edit the already granted explicit, specific and informed consents should be employed to allow users to control the use of their personal data by Data Controllers. Each consent should refer to a specific data set, a specific use of the collected personal data and should clearly state how that data will be used, whether any Data Processors will be provided that data for the noted use and how long the data will be retained.

iii. In order to provide rich customer experience, inter application data transfer should be enabled. This transfer must be compliant with data protection laws.

Q.3 What should be the Rights and Responsibilities of the Data Controllers? Can the Rights of Data Controller supersede the Rights of an Individual over his/her Personal Data? Suggest a mechanism for regulating and governing the Data Controllers

Idea Submission:

- As rightly mentioned in the Consultation Document, a data controller refers to any organization which determines the purposes and means of processing the personal information of users.

- As mentioned in the CP, and based on the report submitted in 2012 by Group of Experts headed by (Retd.) Justice A.P. Shah, Former Chief Justice, Delhi High Court to the Planning Commission on the subject of data privacy, the following can be considered the responsibilities of Data controllers.

  (a) **Notice:** A Data Controller must 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. Such notices should include disclosures on what personal information is being collected; purpose for collection and its use; whether it will be disclosed to third parties; notification in case of data breach, etc.

  (b) **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

  However, as already submitted, for data that is "Anonymized or Aggregated" in nature, and cannot be used to identify a person directly or indirectly, i.e., it is not "Personal information" or "Personally Identifiable information" by nature, there should not be a requirement for any "User Consent". Declarations in respect of such information can be a part of the Organizations' Privacy Policy where the disclosures on what personal information is being collected; purpose for collection and its use; whether it will be disclosed to third parties; notification in case of data breach, etc. should be duly mentioned.

(c) Collection limitation: A data controller shall only collect personal information from data subjects as is necessary for the purposes identified for such collection

(d) Purpose limitation: Personal data collected and processed by data controllers should be adequate and relevant to the purposes for which they are processed. It should, in particular, be ensured that the personal data collected are not excessive.

(e) Access and correction: Individuals shall have access to personal information about them held by a data controller and be able to seek correction, amendments, or deletion of such information, where it is inaccurate.

(f) 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

(g) Security: A data controller shall secure personal information using reasonable security safeguards against loss, unauthorized access or use and destruction

(h) 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 of the data they collect, in order to ensure compliance with the privacy principles. The information regarding said principles must be made in an intelligible form, using clear and plain language, available to all individuals

(i) Accountability: The data controller shall be accountable for complying with measures which give effect to the privacy principles. Such measures must also include mechanisms to implement privacy policies, including training and education, audits etc.

- **It needs to be mentioned here that the TSPs in the capacity as Data Controllers are already taking all necessary steps to protect the privacy of their users. However, a limited mandate is applicable on the other players in the digital ecosystem due to which genuine privacy concerns exist in the case of such entities.**

- **We believe that to fully protect the interests of telecom subscribers, all entities in the ecosystem that deal with personal or sensitive data should be regulated by strong privacy and security laws, and such laws should be equally and uniformly applicable to all the players in the digital eco-system**.

- **<u>Rights of a Data controller Versus the Rights of an Individual over his/her personal data:</u>**
  It is submitted that the rights of a Data controller should supersede the Rights of an Individual over his/her personal data only in the following identifiable circumstances:-

  i. Public emergencies or interests of public safety where such interception is required in the interests of the sovereignty and integrity of India
  ii. Security of the country and for keeping friendly relations with foreign states
  iii. For maintaining public law and order and for prevention of incitement of offences

- **<u>Mechanism for regulating and governing Data Controllers:</u>**

  It is submitted that regular audits conducted by authorized / appointed third party agencies to certify that Data Controllers are complying with privacy regulations can be a mechanism for Data Controllers to identify themselves as 'Privacy certified', and therefore reliable and trustworthy to do business with. Each entity in the ecosystem (telecom or digital), if required to have such a certification on compliance to "Data Privacy Principles", can lead to creation of a much cleaner and safer ecosystem from a privacy perspective.

Q4. 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 consent? 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?

<u>Idea Submission:</u>

- **As already submitted, regular audits conducted by authorized / appointed third party agencies to certify that Data Controllers are complying with privacy regulations can be a mechanism for Data**

Controllers to identify themselves as 'Privacy certified', and therefore reliable and trustworthy to do business with.

- **While it could be difficult to create a technology enabled architecture to audit the use of personal data and associated consent, nevertheless such audits by third party agencies could go a long way in creation of a cleaner and safer ecosystem from a privacy perspective.**

- **However, it is critical that such audits towards use of personal data and associated consents are made mandatory for all the players that deal with personal data in the digital eco-system. However, should the TSPs only be held accountable for such audits, we would strongly recommend that only a self-certification be required of them in view of their proven record.**

- A proactive mechanism to prevent privacy incidents may definitely help minimize harm inspite **of** the varied nature of entities in the different ecosystems in which personal data is collected and used. However, in case of a Data Breach, it is critical that such a breach is immediately reported by the Data Controller/Processor to the users and the government or authorized authority. The onus of reporting such a breach should lie with the Data Controller/Processor.

- Subsequently, the data should be monitored and access to it logged. All access and utilization should be made available in case of an audit requirement. The requirement may arise due to a suspected or actual breach of data security.

Q. 5 What if any, are the measures that must be taken to encourage the creation of new data based businesses consistent with the overall framework of data protection?

<u>Idea Submission:</u>

- As mentioned in the Consultation paper, there is a global trend in the creation of new services on the basis of data. Such services provide significant value to customers and businesses. Incase creation of such new data based businesses is not encouraged, India will fall behind in terms of industrial growth

and development, and the Government's vision of Digital India and Smart Cities would be adversely affected.

- Hence the government must enable this by creating an enabling ecosystem whereby new players are able to bring in innovative services. However, it is extremely critical that the regulatory framework is made applicable on all the players in the digital eco-system to ensure a level playing field among all stakeholders. The measures which can be taken to achieve the creation of new data based businesses are:-

    1. Data Portability which will help extract all user data from one service and share it with another
    2. Creation of public data sets which can be used as a test bed by newer service providers
    3. Business related to compliance and data security will also develop.

Q6 Should government or its authorized authority setup a data sandbox, which allows the regulated companies to create anonymized data sets which can be used for the development of newer services?

<u>Idea Submission:</u>

- The government should make available its own data sets (anonymized) available through its own data, which can enable wider and varied uses of these data sets and result in newer businesses / innovative use cases that can benefit the government as well.

- **However, each entity should be responsible for the data that it owns and there should not be any compulsion on the regulated entities to create anonymized data sets.**

Q7. How can the government or its authorized authority setup a technology solution that can assist it in monitoring the ecosystem for compliance? What are the attributes of such a solution that allow the regulations to keep pace with a changing technology ecosystem?

Idea Submission:

- To set up a technology solution that can assist in monitoring compliance, the following must be considered:-

    i. There are different ecosystem stake holders at play that collect and use data, including personal data. Any compliance regulations should apply to not just the TSP's but any Data Controller in the entire digital ecosystem that directly or indirectly collects or processes personal data.

    ii. Compliance should also be sought from Data Processors (such as resellers & aggregators of telecom services) that may not directly interact with customers and as such may not be held accountable to directly collect user consent

- Given the above, a single technology solution may not serve the purpose of assisting in monitoring compliance. The solutions may vary depending on the business case. A suitable security solution may be designed for each business case. All supporting technologies are available today.

Q8. 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?

Idea Submission:

- The role of telecommunications as one of the key pillars of critical national infrastructure along with the need for preserving data confidentiality make it important to ensure security of telecom infrastructure.

- As rightly pointed out in the Consultation Paper, any vulnerabilities in the telecommunication infrastructure can lead to disruption of basic services which can lead to a severe impact on citizens, businesses and delivery of public services. Hence it is essential to ensure that each layer of telecom infrastructure and the ecosystem as a whole is protected through adequate security measures in

order to safeguard the system. Having said that, the TSPs already have a long history of success in this task, guaranteeing both the privacy of their users and the security of their networks in line with the stringent security conditions, and have invested extensively to have robust security systems in place.

- The following measures can be considered to strengthen and preserve the safety and security of telecommunications infrastructure and digital ecosystem as a whole:-

i. To fully protect the interests of telecom subscribers, all entities in the ecosystem that deal with personal or sensitive data should be regulated by strong privacy and security laws, and such laws should be equally and uniformly applicable to all the players in the digital eco-system including those that offer OTT communication services while using the TSP network / access to reach to the customer with their services.

ii. Directives and legislation by public authorities which ensure availability of services, fair competition and privacy protection would be helpful.

iii. As per Section 70 of the Information Technology Act 2000, there is a provision for declaration of certain areas as critical information infrastructure (CII) and the need for introducing appropriate measures for the security of these systems. Keeping in view the critical role of the telecommunications sector, the National Critical Information Infrastructure Protection Centre (NCIIPC), the agency mandated to facilitate protection of critical infrastructure has designated telecom as one of the CIIs

iv. Telecommunication infrastructure linked with private/hybrid clouds must have enhanced security protocol and fail safes so as to ensure better security of data and avoid data theft.

v. For the digital ecosystem there is need of application data storage monitoring mechanism and the application owner should be bound by governmental data security norms

Q9. What are the key issues of data protection pertaining to the collection and use of data by various other stakeholders in the digital ecosystem, including content and application service providers, device

manufacturers, operating systems, browsers, etc? What mechanisms need to be put in place in order to address these issues?

Idea Submission:

- The key issues of data protection pertaining to the collection and use of data by various other stakeholders in the digital ecosystem, as rightly pointed out in the Consultation Document, can be summarized as below:-

  a**. Tracking users through cookies and fingerprinting** – Cookies or small files which allows a website to identify a user's device. As per research, users have a low level of awareness about the meaning and use of cookies and the beneficial and harmful objectives for which they can be deployed

  b. **Device Fingerprinting** – This method uses various information elements transmitted by a device in order to identify it. Different software, platforms and APIs each offer access to different information elements stored in the device

  c. **App Permissions** – While increasing use of apps designed for specific purposes like entertainment, banking and payments, email and communications etc offers many efficiencies and benefits to both users and developers, they also pose several concerns from a data protection perspective by allowing an app owner to collect vast amounts of data about the user. Apps may also collect information about other people (who are not their customers) through a consenting customer. For example, global directories of phone numbers crowd-sourced through customers. The person whose personal information is being shared may not be aware of this sharing. Further, other players in the app ecosystem like app stores, operating systems, device manufacturers and other third party like analytics and advertising providers also play a critical role in collecting and processing personal data through apps.

  d. **Control by Devices** – The devices and equipment used by individuals to connect to various networks also have the ability to gather large volumes of data about the user's behavior. In addition to this, the growth in the adoption of Internet of Things (IoT) devices also raises concerns about the nature and extent of data being collected by these devices.

e. **Aggregators -** Aggregators refer to the companies that aggregates SMS and other telecom service capabilities and provide these to enterprises. These entities have the capability to read the A2P SMSs being sent to the users and can store the information. Since there are no regulations that govern them, they can potentially share this information with other data processors who can further monetize this data.

- **Typically, TSPs are liable and responsible for a plethora of licensing provisions and regulations that include, regulatory levies and license fees, QoS, Tariff Regulations, confidentiality of customer information, Regulatory Audits, Consumer Protection Regulations, emergency services, privacy of communication and lawful monitoring and interception. These conditions are not imposed on unlicensed OTT players or the other players in the digital ecosystem that process and control the personal data of users such as content and application service providers, device manufacturers, browsers, operating systems, etc. These players thus sit outside of licensing conditions and are not burdened by multiple historic obligations that currently apply to TSPs thereby posing social and economic risks of lower consumer protection / data privacy and security approaches which do not reflect the national telecom policy.**

- **There is thus a need for an overarching framework/legislation that addresses comprehensively the definition of Personal Data and its protection mechanism, and reaches out beyond the TSP's to include all organizations and entities in the digital ecosystem that are involved in collection, processing and usage of personal data.**

Q10. Is there a need for bringing about greater parity in the data protection norms applicable to TSPs and other communication service providers offering comparable services (such as Internet based voice and messaging services). What are the various options that may be considered in this regard?

Idea Submission:

- As already submitted, TSPs have various requirements for data protection of users imposed on them both by sector specific laws (Indian Telegraph Act 1885, Indian Telegraph Rules 1951, initiatives and

directives of TRAI) as well as the general provisions and conditions of Indian IT Act 2000. On the other hand, many of these conditions are not imposed on unlicensed OTT players offering communication services that sit outside of licensing conditions and are thus not burdened by multiple historic obligations that currently apply to TSPs. Naturally, the telephony services delivered through such OTT application routes are plagued with multiple issues such as:

i. **Custom build nature of applications**: These applications are custom build solutions of individual operators and therefore cannot be universally applied across all networks.

ii. **Compliance with all security norms**: Such applications cannot not meet all security norms, including voice mentoring and location information as is mandated for any licensed telephony services today.

iii. **Provision of emergency call routing**

iv. **Performance issues on account of service priority**: Owing to its real time nature, telephony service is always given priority over any data service. However in case of OTT based applications, no priority can be provided leading to performance issues.

v. **Constant tuning of applications**: It is not always guaranteed that the application will work in a hassle free manner without any issues with every operating system (OS) upgrade. Thus, constant tuning of app may be required.

vi. **Threat of security breach**: Registration process to identify the customer may not be fool proof thus can be a security breach without any proper audit trail.

- **It is important to note that reliability of Telephony services are most critically viewed when it comes to data security / protection / privacy / confidentiality of the users. No abuse in this respect should be allowed merely on the basis of commercial levers.**

- **It is thus only appropriate that OTT players offering comparable communication services be urgently brought under a suitable Regulatory framework that imposes upon them the same obligations that apply to TSPs in respect of data security / protection / privacy / confidentiality, and results in regulatory parity.**

Q11. What should be the legitimate exceptions to the data protection requirements imposed on TSPs and other providers in the digital ecosystem and how should these be designed? In particular, what are the checks and balances that need to be considered in the context of lawful surveillance and law enforcement requirements?

Idea Submission:

- The principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is no longer identifiable.

- The legitimate exceptions to the data protection requirements imposed on TSPs and other providers in the digital ecosystem should also be based on the following identifiable circumstances where national/public interests come before individual interests for data protection. They are:-

    1) Public emergencies or interests of public safety where such interception is required in the interests of the sovereignty and integrity of India
    2) Security of the country and for keeping friendly relations with foreign states
    3) For maintaining public law and order and for prevention of incitement of offences

- In the context of lawful surveillance and law enforcement requirements, there needs to be a clear demarcation and definition of what information can be accessed for that purpose. The procedures and permissions relevant to such surveillance must also be clearly laid down by the authority.

Q.12 What are the measures that can be considered in order to address the potential issues arising from cross border flow of information and jurisdictional challenges in the digital ecosystem?

Idea Submission:

- In today's global world where businesses spread across geographies, it is very important to address the issues arising from cross border flow of information and jurisdictional challenges in the digital ecosystem without compromising on the requirements of innovation, efficiency and security.

- For eg, in many cases, global companies operating in India, may have their data servers located in their home nations. An example of this certain Chinese device manufacturers which control a significant share of the handset market in India. In such cases, it must be made clear to these businesses that all information pertaining to their Indian customers is handled in a safe, secure manner which is subject to audit by relevant regulatory authorities. The same has been initiated by Government of India as per their recent order to these device manufacturers to disclose details about the procedures and processes they follow to ensure the security of mobile phones sold in India, following reports of data leakage and theft.

- To address the issue of access to data, hosted by CSPs in different jurisdictions, by law enforcement agencies, we note that the TRAI in its recommendations on cloud Computing, has already recommended that:
  i. Robust MLATs should be drawn up with jurisdictions where CSPs usually host their services, enabling access to data by law enforcement agencies
  ii. Existing MLATs should be amended to include provisions for lawful interception or access to data on the cloud.

- We recommend that a similar approach may be adopted in respect of jurisdictional challenges pertaining to cross border flow of information in the digital ecosystem.

- Additionally, there can be an Artificial Intelligence and Machine Learning enabled architecture implemented by the Government to intercept and analyze any cross border data exchange. This will enable the Government to track and prevent any malicious/fraudulent data being shared across two different entities in different geographies.