EXOTEL'S RESPONSES TO THE CONSULTATION PAPER ON PRIVACY, SECURITY AND OWNERSHIP OF DATA IN THE TELECOM SECTOR

EXECUTIVE SUMMARY

1. Definition of personal data to include data subject's web browsing history across devices, app usage history, communication content, devices' precise geo-location, children's information, social security numbers such as Adhaar card number, voter id card number, passport number etc.
2. The data subject should have the legal right to control the use of his/ her personal data.
3. Data controller should be allowed to collect, use, process and transfer personal data subject to:
    a. The data controller notifying the data subject of the exact scope of personal data it needs to collect; purpose of acquiring such personal data (which should be legal, fair and directly related to service/ product being availed by the data subject)
    b. The data subject granting an affirmative opt-in consent
2. The Data Protection Authority should prescribe a standard form for the requisite notice and consent for collection, use and/or transfer of personal data. The standardized form will make it easier for consumers to understand and stop the use of confusing language
3. A Data Protection Authority should be created which, amongst other things, develops a platform for (i) registration of data controllers; (ii) monitoring compliance with revised data protection regulation. This platform can be developed through a PPP model.
4. The data controllers should be required to notify breaches of privacy, data security regulations and standards within a prescribed time period.
5. Violation of data protection regulations and privacy of data subject should be deemed a serious offence and attract hefty penalty as well as the compensation to data subjects.

Question 3

What should be the rights and responsibilities of the data controllers? Can the rights of data controllers supersede the rights of an individual over his/ her personal data? Suggest a mechanism for regulating and governing the data controllers?

We would define a data controller as anyone who has access or ability to process the personal data of an individual. Telecom service providers (TSP), internet service providers (ISP), intermediaries including search engines, social media website, software as a service provider, communication solutions, e-banking portals, digital payment portals and applications, e-commerce portals and applications should all be called Data Controller.

Unfortunately, there is misuse of customer information and data for commercial purposes. Business practices of a few, who exploit consumers through various psychological and behavior information of the consumers, erode the trust of customers on new technologies. Also, the existing "take-it-or-leave-it" terms of consent forces the consumers to bear all the risk.

Hence, we feel it's necessary that strong steps be taken to not only to protect the consumers but also to foster trust in new technologies and businesses.

The first step to clearly define scope of personal data. The following should be a part of the definition of personal data

1. Financial information
2. Caste, religion, sexual orientation
3. Medical records and history
4. Biometric information
5. Web browsing history across devices
6. App usage history
7. Content of the person's communication
8. Geo-location
9. Social security numbers - *Adhaar* , voter id, passport etc
10. Derivatives which can include personal preference and habits inferred or identified from personal data

Our recommendations on rights and obligations of data controllers will revolve around prevention of misuse as remedial measures are impractical because of the following reasons:

i. Difficulty in tracking cyber criminals: - It is difficult to track down the perpetrator (i.e., an individual or entity) of a cybercrime due to use of alias and IP masking
ii. Difficulty in apprehending cyber criminals due to jurisdictional problem: The cybercriminal could be based out from any countries including the ones which are hostile to India
iii. Failure to getting physical hold of cybercriminals in a way encourages them
iv. Difficulty in loss mitigation: - Any personal data shared while using services of an application or portal (especially if the service is on the cloud) gets copied over and over on the web in a short amount of time. Even if removal of such data is attempted,

one cannot be sure that all of one's personal information has been completely removed off the web.

A data controller should have the **right** to collect and process personal data only when

i. The data subject has explicitly and knowingly granted his or her consent in favour of such collection and processing, after being adequately informed through a notice by the data controller;
ii. Data processing is needed for a contract, for example, for billing, a job application or a loan request;
iii. Processing of group level (not individual level) will help improve the services offered to data subjects
iv. Transfer of data only to enable fulfillment of the service. Say, an e-commerce company can pass on the phone number of a customer to a cloud telephony company to inform the customer of the status of order
v. Processing is required as per applicable law

Every data controller should be under an **obligation** to

i. Collect, process, use and/ or transfer personal data only legally and fairly for explicit and legitimate purposes. The personal data so collected should be relevant and not excessive in relation to the purposes for which it is collected and/or further processed.
ii. Make easy, accessible and visible provisions for data subjects to rectify or remove incorrect data about themselves and/ or their personal data.
iii. Explicitly state the expiry period for stored personal information. Personal data should not be kept any longer than is necessary. And hoarding of personal information should not be encouraged
iv. Protect personal data against alteration or unlawful disclosure. They should be required to maintain appropriate security measures
v. Respond and resolve complaints regarding breaches of data protection effectively and in a time bound manner. Perhaps, 2-tier grievance redressal system with QoS should be established
vi. Notify the customer/ data subjects about any data breaches and any reasonably suspected or anticipated data breaches.

Rights of a data controller vs. the rights of a consumer: The legal ownership and control of personal data should at all times remain with the individual to whom such personal data relates to.

A mechanism for regulating and governing data controllers

i. ***Data Protection Support and Monitoring Authority:*** A data protection support and monitoring authority whose functions and responsibility will be
    a. **Providing a platform** for registration of stakeholders and monitoring compliance with data protection laws
    b. **Investigating** data breaches and complaints regarding personal data by Data Subjects**:** The Data Protection Authority should have the powers to decide the complaint and have the power to
        i. Direct the data controller to do or omit to do something

ii. Impose a monetary penalty on the data controller based on the sensitivity of the underlying data
iii. Suspend or shut down the services of the data controller upon the gravity of the data protection violation

ii. **Registration:** All data controllers should be required to register themselves as data controllers. The registration should be classified depending upon the scope and nature of the business.

iii. **Notification:** Every data controller should notify the Data Protection Authority of the purposes for which it collects, uses and/ or processes personal data and/ or proposals to do so. Having a clear and transparent notification process will deter data controller from collecting excess information

iv. **Registration of choice of Data Subjects:** The data subjects should also be able to modify their preferences through a call, message and/or by logging in to the Platform through a registered id and password. The following feature should be available to data subjects :-
    i. completely prohibit the use of their personal data (except for purposes defined under any applicable law);
    ii. specify additional purposes for which they wish to allow use of their personal data

Who can collect, principles of collection, use and transfer of personal data, prescribed form of notice, opt in consent, transfer consent etc.

i. **Registered data controller:** Only a registered data controller should be allowed to collect, use, process or share (with other registered data controllers) personal data.

ii. **Purpose:** The purpose for collection of the personal data should be directly related to the service and/ or product being offered by the data controller to its customer/ Data Subject

iii. **Standardized notice**: The Data Protection Authority should prescribe a format to prevent the consumers being confused by complicated language of notice about the use of personal data. This format should include
    a. The list of data points being collected
    b. The purposes for collection of personal data
    c. A list of third party registered data controllers (say payment gateway, communication provider-sms, voice, ticketing platform for complaint management) with whom such information may be shared and the purpose for such transfer
    d. The duration for which such personal data will be stored

iv. **Consent:** The Data Protection Authority should prescribe a format to prevent the consumers being confused by complicated language of "Terms of consent". This consent Form should also enable the Data Subject to specify the duration for which the affirmative Opt-in Consent has been given by such Data Subject, the limited purpose of the consent and state the date as to when data will be deleted

v. **Transfer:** A data controller should only be able to transfer personal data to a registered data controller listed in the notice and the terms of consent.

vi. **Collection of personal data for a contract** (example billing, a loan request etc) Collection of minimum personal data such as email, telephone number, age, bank statement for

specific contractual purposes (eg. billing, insurance application or a loan application) should be permitted. Also,

a. The transfer of data should not be permitted for any unrelated purpose
b. personal data collected for such purposes should be automatically deleted within the prescribed period and/ or upon termination of the contract

vii. **Processed as per applicable law:** Where data collector gathers personal data from a consumer/ Data Subject under an applicable law, then the Data Subject should be notified about the particular law in the Notice. personal data collected under this category should not be retained by the registered data controller beyond the period of time specified by the law. Data controller should not be allowed to share such category of personal data with any third party for commercial benefit.

viii. **Alternation & deletion:** The data controller should provide a mechanism for the Data Subject to change his preference.

a. The change of preferences should be implemented within 7 working days.
b. Where the Data Subject has opted-out, the data controller should delete the concerned personal data within 7 working days.
c. Where the contract of service is such that the personal data cannot be deleted immediately, the Data Subject should be informed accordingly in writing or via email.

ix. **Complaint handling and resolution:** All data controllers should have a complaint handling system, details of which should be uploaded against its registration number on the Data Protection Authority's Platform and its own platform. In case of any unresolved disputes, the data protection laws should provide an escalation system through the authority's Platform.

x. **Handling Complaints by Data Protection Authority:** Data controllers must respond to any complaints received regarding misuse of data under their control within 5 working days. If a Data Subject believes that his/her rights have been breached or that his/her personal data has been compromised, he/she should have the right to request the data controller to remedy the situation. If the complainant Data Subject does not receive an adequate answer from the data controller within 15 days, he/she should be able to escalate it to the Data Protection Authority. If the personal data concerned is found to be inaccurate or to have been unlawfully obtained, the Data Subject should have the right to demand that it be corrected, blocked or erased and s/he be compensated for the harassment or injury or loss.

xi. **Security standards:** Registration on the Platform should be linked to meeting the prescribed data protection and security standards. The standard certification for data security requirements should be incentivized.

Questions 1 and 2

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?

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?

The issues of concern in Questions 1 and 2 are closely inter-related and in our view Question 2 is a corollary of Question 1, therefore we will attempt to respond to both questions together.

Existing data protection framework and unsatisfactory industry practices

The existing laws gives room to data controllers to hoodwink their customers/ Data Subjects into providing them consent for collection, use, processing and transfer of all of their personal data shared with the data controller. Some of the practices in the industry that stand in the way of establishing Data Subject's right over their personal data; and could be changed through amendments in law and effective implementation, have been briefly discussed under:

i. **Disclosure of personal data:** In practice, data controllers seldom provide notice or take an affirmative opt-in manner of consent before collecting, using, processing and sharing/disclosing the personal data of their customers/ Data Subjects. The 'disclosure' to say, is made in the privacy policy and terms of service, and the links to these legal documents are generally kept in the least accessed part of the application or web-portal as the existing law does not make data controllers responsible for ensuring that the customers/ Data Subjects actually read and understand these documents and their implications.

   Usually the privacy policy is placed on the application or web-based portal in such a manner, that the customer by-passes this privacy policy document and goes on to access the internet or services, unaware of the kind of personal data being collected and/or how it will be used by the data controller. Secondly the privacy policy typically states that by accessing and using the website, the consumer/ Data Subject gives his/her automatic consent to their privacy policy.

ii. **Choice and consent:** The law on informing the Data Subject and taking his/her consent for collecting, processing, using and sharing their personal data appears to have been contorted by some data controllers to their advantage. Their terms of service are "take-it or leave-it" in nature. Such terms of service are generally worded in the following manner *"By accessing or using our website, you are agreeing to these terms of service … You may not use the services if you do not accept the terms of our service" or "by accessing and using the website, the consumer gives his/her automatic consent to our privacy policy and terms of use".* Therefore in effect, a customer/ Data Subject is forced to accept the terms of the privacy policy and terms of use, even if the collection of a particular type of personal data may not be directly related to the services that a customer/ Data Subject may be accessing or availing. This also means that some data controllers refuse to serve customers who don't consent to the use and sharing of their information including personal data for commercial purposes or otherwise.

iii. **Collection limitation and purpose limitation**: It was recommended that a data controller shall only collect personal information from data subjects which are adequate and relevant to the purposes for which they are processed.

   a. In today's information economy, the "*take-it or leave-it*" privacy policy and terms of use should not be used to gather excess personal data and exploit them for commercial gains. The industry has not been able to self-regulate or arrive at standard industry practices that limits collection and purpose of collection/use of personal data. Principles of collection limitation and purpose limitation are being undermined which puts customers/ Data Subjects' privacy at risk. Hence, there is a need for regulation.

iv. **Security Standards:** The law requires a data controller to ensure that it has 'reasonable security practices and procedures' (hereinafter the "**Security Standards**"). However, from a data subject's point of view, there is no visibility on what kind of security standards a data controller has in place; or whether the security system is effective enough. Reporting/ publishing of security standards compliance on the webpage or application should be made mandatory by law.

v. **Data Breach:** Often the data controllers hesitate in taking or do not take steps to inform customers/ Data Subjects on time, fearing loss of reputation or other commercial considerations, thereby putting the security and protection of their customer/ Data Subject's privacy on the back burner.

Therefore, it is clear that although there is a legal framework governing data protection and security systems in existence, however in view of the advancement in technology and our dependence on the digital ecosystem, there appears an obvious and sizable lag between the advancement of technology and the amendments of the law. The data protection requirements currently applicable to all the players in the digital ecosystem are insufficient to protect the interests of telecom subscribers. Therefore, we propose the following suggestions to tighten the existing data protection framework from the point of view of the Data Subjects.

Suggestions

i. **Expanding the definition of personal data:** As stated in our response to the previous question, the definition of the term personal data should be expanded

ii. **Notice in standardized format:** The data controller should mandatorily flash the notice only in the prescribed format before allowing access to website or application. Such a Notice list personal data being collected, the purpose and the list of third party registered data controllers with whom such information may be shared.

iii. **Options to give consent to collect none, some or all personal data shared with data controller:** By default, each category of personal data should be disabled in the Consent Form. Only when the customer/ Data Subject expressly agrees to each category of information, should the data be collected.

iv. In case of **revision of terms**, the data collector should automatically expunge all the personal data related to the customer/ Data Subject that it had stored if the customer does not give opt-in consent.

v. **Prescribe basic minimum template for Notice and Opt-in Consent:** The Data Protection Authority should create standard templates for giving notices to, receiving the opt-in consent from, receiving revisions in consents from the customer/ Data Subjects mentioned in these responses.

vi. **Responsible sharing of personal data.** Transfer of personal data should be allowed only under the following terms
    a. The transfer of personal data is necessary for providing the service to the customer
    b. only to registered and listed [in the notice] third party data collectors

vii. **Intimation upon breach - actual, suspected or anticipated:** The data controller should intimate the customers/ Data Subjects and the Data Protection Authority within 48 hours of breach - actual, suspected or anticipated.

viii. **Mandatory enquiry into the cause of the breach**: In the event of an actual breach, an investigation by the security expert should give its findings and recommendations to plug the reason for the breach and submit the same with the Data Protection Authority. The recommendations should become a public document. The references to manner of operations and reference to any intellectual property or proprietary technology of the data controller may be redacted before releasing the document in public. The data controller should be required to send a report within three months, stating how the cause for breach has been plugged.
    If such an investigation reveals that the data controller did not take action, even though he had reasonable knowledge to suspect the breach of personal data and did not notify the customers/ Data Subjects immediately on having such knowledge; or the data controller had reasonable knowledge of such a breach and was also in a position to remedy the breach if actions had been taken in time, then there should be a heavy penalty on such a data controller and/or suspension of their services. Strict penalties will encourage the data controllers to maintain high security standards and minimize the data breaches in the future.

ix. **Platform for registration of stakeholders and monitoring compliance with data protection laws:** The proposed Platform can be developed by way of a public private partnership.

Question 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?

The On-cloud economy is based on sharing servers. To ensure reliability and very high uptimes, the infrastructure provider decides the location of server farms on many factors including the location being a seismic safe zone, size of accessible market. Hence, flow of data across borders is inevitable.
Blanket restriction of flow of information across border is a myopic solution. Such restriction would deny Indian business the flexibility, cost competitiveness and reliability of the Cloud.
Instead, the regulator should focus on strengthening India's extraterritorial jurisdiction and the cross-country cooperation over data protection.

Strengthening India's extraterritorial jurisdiction over data protection issues: Currently, the Information Technology Act ("**IT Act**") in India provides for some measures relating to data protection and has an extra-territorial reach. However, the extra-territorial applicability aspect of the IT Act should be further clarified and strengthened by expressly including the following measures:

i. India should assert its jurisdiction over a dispute about information/personal data held on the cloud when either the parties (data collector/data subject) or the subject matter of the dispute has a "real and substantial connection" with India. By "real and substantial connection", we mean that the information/personal data is (i) collected from consumers/data subjects residing within India ("Indian Consumers/Data Subjects"); and/or (ii) collected, stored, used or processed in India; and/or (iii) disclosed by a party in India; and/or (iv) disclosed in the course of a commercial activity carried out in India. The term "course of a commercial activity" should be defined to include an activity directed at advertising or promoting a service to Indian Consumers/Data Subjects.

ii. India's jurisdiction should be extended to any cloud-based service provider/data collector (based in a foreign country) who is "present" in India. A data controller/cloud-based service provider should be deemed to be 'present' in India if (a) it has a subsidiary, branch office, liaison office or project office in India; or (b) has conducted continuous and systematic business in the territory of India for a reasonable period of time; or (c) is present in India in any other form whether through agents/ intermediaries or otherwise.

iii. Indian law should also be applicable to such a foreign data collector/ cloud-based service provider whose services have been used to carry out actions, be it anywhere in the world that adversely affects commerce in India.

Creating Global Data Protection Provisions: India should sign treaties with the countries where the major server farms are located to ensure applicability of Indian data laws for data of Indian users.

Question 4 & 7:

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?

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?

There should be clear guidelines on what is not accepted. Such guidelines will protect the startup community from unintentionally overstepping the boundaries.

There are more than one billion telecom subscribers, each of whom might subscribe to one or more services. There will be a couple of billion touchpoints. Having a technology solution is the only way to monitor the ecosystem for compliance. However, with the complexity &

diversity of technologies being used, human intervention is required. Human intervention in all cases will both be costly and create a huge competition for smaller number of capable auditors. Hence, we suggest a mix of technology solution to keep the cost of compliance low and human audit to handle complexity and evolving technologies

i. Basic technology based test suite to check the hygiene security & audit requirements. This suite should also suggest basic recommendation if the product fails this test. This technology audit will also reduce the workload for human auditors
ii. Build a team of "white hats" or human auditors. These auditor will check only for exceptions as the hygiene requirements have already been vetted.
iii. With the auditor completing the tests and setting benchmarks, compliance is a matter of adhering to the benchmarks. Hence, compliance monitoring should be fully automated with a technology based solution.

The regulators should get into a public private partnership & promote solution to come from the ecosystem. The regulator only needs to manage the requirements while the ecosystem will finds a way to keep pace with evolving technology.

Again, audit alone will not suffice. Financial liability for misuse of personal data, especially in critical sectors (finance, health), should be placed to demotivate such misuse.

Question 5 & 6:

Q5. 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?

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?

Exotel would not like to trade its user data with third party even as anonymized data sets. We believe, this is a breach of user privacy and our confidentiality agreement with clients. We should not underestimate the consequences of sharing personal or impersonal information over an extended period of time.

i. It is possible to derive fairly accurate information on consumer's behaviour [personal information] from impersonal information which the consumer consented to share.
ii. It is possible to combine partial information from two different sources to reveal extremely personal information.
iii. Even with anonymized data sets it is possible to identify vulnerable user groups and they can be exploited for disproportionate commercial gains.
iv. In B2B environment, sharing of user data would lead to trading competitor information.

Hence, we recommend against that the government setting up data sandbox.