**8 September 2017**

To,
The Telecom Regulatory Authority of India (TRAI)
Mahanagar Doorsanchar Bhawan
Jawahar Lal Nehru Marg
New Delhi-110002

**Subject**: Response to the consultation paper dated 09th August 2017 on Privacy, Security and Ownership of the Data in the Telecom Sector

Sir,

This response letter to the consultation paper dated 09th August 2017 is being submitted by MakeMyTrip (India) Private Limited (hereinafter "MMT").

MMT is one of India's leading online travel agencies that facilitates bookings for its customers of various travel products and services like flight tickets, hotel rooms, holidays, train tickets, bus tickets and car bookings. It operates through its website www.makemytrip.com, its mobile applications and various retail stores across India. The customers of MMT share their personal information to MMT for the purpose of getting their travel related bookings facilitated and confirmed. Such personal information may include name, gender, email id, mobile number, address and certain payment related information like card details etc. MMT has strict procedures and controls in place to secure such personal information and uses it only in the manner as consented by the customer. As a collector and processor of data of its customers, MMT submits the following in response to the questions raised in the consultation paper.

**Question No. 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?**

**Response:**

The important regulations in India which have certain sections towards protecting the data and privacy of individuals are:

1) The Indian Telegraph Act, 1885;
2) Information Technology Act, 2000; and
3) Regulations formulated by TRAI from time to time

Despite the above, there are various instances of data getting breached in India in forms of:



MakeMyTrip (India) Private Limited CIN - U63040DL2000PTC105210 | www.makemytrip.com

Corporate Office Address
19th Floor - Tower B, Building No. 5 (Epitom),
DLF Cyber City, DLF Phase III, Gurgaon 122002

Registered Office Address
UG-07, Front Side, TDI Mall, Rajouri Garden, New Delhi-110027
Telephone No. +91 124 439 5000 | Fax No. +91 124 439 5100

1) Telecom subscribers getting promotional text messages and cold calls despite listing their phone numbers in the NCPR;
2) Various instances of customer's contact details being sold by entities collecting such data from individuals on the pretext of marketing or selling some product or service;
3) The banking or credit card information of the customers being leaked by the collecting entities (like a hotel, a merchant, an e-commerce platform etc.) either knowingly or inadvertently;
4) Hacking into the systems and website of the entities which have customers' information and divulging that data to third parties for illegal gains.

The above instances indicate that there is a necessity for a more robust regulatory framework in India for protecting the data of individuals, and a mechanism to enforce the same. The constant growth and evolution of the digital eco-system makes it mandatory for such regulatory framework to be updated from time to time.

With the above background, we suggest that the Government of India may frame more elaborate regulations to protect the interest of the telecom subscribers generally, and to also protect the privacy of data of individuals. The volume of data being handled and the manner in which such data is being used vary from industry to industry; therefore, the regulations have to be customized for each industry like banking, telecommunication, electronic commerce, travel agents, merchants, hotels, payment gateways etc.

**Question No. 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?**

**Response:**

The definition of "personal data" as provided under The Personal Data Protection Bill 2014 is broad enough and can be considered by the regulator. Further, "sensitive personal data" is defined in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. The extent and purpose of these definitions is sufficient in the current scenario.

The User's consent should be taken before sharing his personal data for commercial purposes.

However, the regulations have to clarify what is a "commercial purpose". In our understanding, a "commercial purpose" shall mean usage of individual's data for purposes other than the transaction for which the individual has shared his data.

For example:

1) User booking a flight ticket on an online portal of a travel agency consents that his contact details may be shared with the respective airline for it to update the customer about the flight status, delays etc. So, when the travel agency shares the contact details of the customer with the airline, it is purely for transactional purposes and shouldn't be considered as a "commercial purpose".
2) A Users may consent that the Data Controller may use their data for providing personalized experience to them whenever they log into their account with the above Controller or uses its mobile. It should be considered a part of the transaction and thus not a commercial purpose.
3) While creating an account with an e-commerce portal, a User provides contact details and also consents that the portal may send marketing communications or any promotional offers from time to time, either through email, phone or text messages. In this scenario, the portal sending such marketing or promotional communications cannot be called "commercial purpose" as the User has offered the contact details to be used by the portal as above. However, if the portal shares the User's data with any third party for purposes other than what the User has consented, then such sharing should be "commercial purpose".

The regulations should also clarify what are the various ways in which the consent can be obtained. Taking consent from a User before each instance of sharing such User's data would be an onerous obligation on the Data Controller, and will only annoy the User with repeated requests for consent. So, a one-time consent from the User when he/she shares data with the Controller for the first time should be sufficient, provided the User should always be given the choice to retract his consent prospectively, or limit such consent only to certain specified types of sharing of data. This empowers the Users to own and take control over his personal data, and also specify the terms of usage of their personal data.

It is pertinent to note that all well-established service providers handling customer data have set processes whereby user consent is taken prior to obtaining the data and the option to opt out of services is also given to users by such service providers. MMT has such processes in place and it also gives the Users an option to opt out of our promotional campaigns at any time.

**Question No. 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.**

**Response:**

Firstly, the regulations should clearly define the terms like Data Controller and Data Processor. In general parlance:

1) Data Controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

2) Data Processor is a person who processes data on behalf of a data controller. A data controller decides the purpose and manner to be followed to process the data, while data processors hold and process data, but do not have any responsibility or control over that data.

Data Controllers should:

1) Take consent of the Users before at the time of sharing data;
2) Ensure that such consent mentions:
   a) The purposes for which the data will be used. This may include sending promotional messages to the Users over text messages, emails or phone calls, and
   b) The nature of the third parties with whom the data will be shared.
3) Provide the Users the choice to retract their consent prospectively or to limit the consent to only certain specified types of usage and sharing with third parties.
4) Share data of Users only with such Data Processors who have reasonable processes in place to protect the data of the Users and to prevent any misuse.

However, the Data Controllers cannot be made liable for breach of data privacy by persons whom the data is shared as a part of the specific transaction made by the User. For example:

1) An online travel agency may have to share the User's contact details with the airlines, hotels, transport vendors or such other suppliers whose product or services the User has booked through that travel agency.
2) An e-commerce platform may have to share the User's contact details with the logistics partner who will deliver the product bought by the User, or the vendor who has actually sold the product.

Making the Data Controllers liable for any breach of data privacy by the airlines, hotels, transport vendors, suppliers, sellers or logistics will be very onerous and will be detrimental for the furtherance of the Digital India vision of our Government which actually encourages electronic mode of transactions and payments. Also, the above entities with whom the data is shared cannot be called Data Processors engaged by the Data Controller for the reason that such entities are not supposed to 'process' the data of the Users but only use such data only for the limited purpose of the transaction.

If such entities misuse the data, then the liability should be only of the respective entity which has misused it rather than the Data Controller which has shared it after obtaining the User's consent. In other words, the source of data breach has to be identified and depending on from whom and for what purpose that source has received the data, the liability has to be established.

**Question No. 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 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?**

**Response:**

Given the current size and volume of the businesses in India which handle data of Users, it may be impractical to form a government owned body which will audit the usage of personal data and the associated consents. Rather, the regulator may create certain minimum standards which are to be followed by Data Controllers and Data Processers, and such Controllers and Processors should get a third party independent audit conducted on their systems. For example, reference may be taken as to how the investors in India rely on the credit rating of CRISIL or similar rating agencies before they consider investing into any stock or debentures of an offering entity.

Such audit based mechanism will provide sufficient visibility for the government or its authorized authority to prevent any harm to User data. As explained above, there is no necessity to create new work-force of auditors to take these responsibilities. The regulator has to prescribe the minimum standards of data protection which the Controllers and Processors should follow, and they will further get their processes audited by an independent and reliable third parties who already exist in the market or may evolve further. Certifications from bodies like PCI DSS, ISO etc. are some examples of independent third parties who are already existing in the market. The scope of audit should include various aspects like:

1) Is the business entity collecting only such data which is absolutely necessary for its business?
2) Are the terms of service clearly worded to explain the manner in which the data will be used, the persons to whom the data will be shared?
3) Is the consent of the User obtained before the data is collected?
4) Does the User has the option to retract his consent, or to change its terms to broaden or narrow it; and does the business entity follow such revised consents?
5) Is the system, website, infrastructure and the security framework of the business entity strong enough to prevent of hacking, cyber-attacks, attacks by ransomware or other forms of data leakage or harm.

**Question No. 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?**

**Response:**

Everyone who is dealing with customers at large is in possession on their respective User's data and such businesses are based on the data so collected from the Users.

So, it's not clear if the question is indicating about businesses which deal only with data collection and its sharing with third parties, and accordingly such businesses have no product or service to sell. If the question is regarding such businesses, then in the current Indian environment the data based business are still evolving. If the regulator intends to encourage the creation of such data based business, then such business have to be highly regulated to make sure that they don't trespass the consents provided by the Users from time to time.

**Question No. 6**

**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?**

**Response:**

We suggest that a strong regulatory framework which defines minimum protection standards coupled with a mandatory periodical third party audit or certification are adequate to protect data privacy in India. Creating a data sandbox may actually be relevant to only some specific businesses which don't need personally identifiable information; accordingly, this may not be a worthwhile effort.

**Question No. 7**

**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?**

**Response**:

The response to query number 4 above, may be considered as a response to the aforesaid query as well.

**Question No. 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?**

**Response:**

MMT skips this question as it is relevant to telecommunications industry. However, question no. 4 already answers the measures to be taken to preserve the digital ecosystem as a whole.

**Question No. 9**

**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?**

**Response:**

The following is the illustrative list of various stakeholders in the digital ecosystem who have access to, or who store or process User's data:

1) Original equipment or device manufacturers (like Apple, Samsung, xiaomi etc.);
2) Telecom companies, data provider (ISP) (like Airtel, Vodafone, Nextra etc.);
3) Operating system provider (e.g. Android, iOS);
4) App platform (e.g. Google Play store, Google);
5) App developers/service providers (like many e-commerce companies);
6) Third parties that support one or more of the above members (e.g. Payment gateways, Analytics service providers etc.);
7) Browsers like Chrome, Safari.

Currently, data protection requirements are not fully applicable to all players in the ecosystem. Therefore, the solutions suggested in answers to question no. 4 are very much applicable to all the above stakeholders.

**Question No. 10**

**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?**

**Response:**

MMT skips this question as it is relevant to telecommunications industry.

**Question No. 11**

**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?**

**Response:**

The legitimate exceptions should include:

1) Data shared pursuant to and within the limitations of the User's consent;
2) Disclosures pursuant to any judicial inquiry or audit process;
3) Storage of data to comply with the applicable laws like Companies Act, 2013;
4) Absolving the Data Controller from the liabilities due to breach of data privacy by the ultimate service provider or the product seller to whom the data is shared by the Controller as a part of the transaction made by the User;

5) Disclosure required in any litigation initiated by or being defended by the Data Controller or Processer against the Users.

The above exceptions may offer some of the checks and balances for enforcement of the regulations.

**Question No. 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?**

**Response:**

In the current global scenario, businesses in various countries engage with each other for services or products. For example:

1) An e-commerce company may procure the product bought by the User from an overseas vendor;
2) A travel agency has to share the User's data with an overseas hotel the room of which the User has booked for stay;
3) A business in India may engage with an overseas vendor for monitoring of fraud or keeping the website secure from infiltration;
4) Engagement of overseas payment gateways by entities which have operations in India.

It is therefore impossible to block cross border sharing of User's data. On the contrary, cross border flow of information is very important for growth of Indian business. However, the flow of such data has to be regulated to ensure that:

1) The User exercises control over their data, its usage and sharing by the business entity;
2) The business entity has the necessary framework to ensure that the user data is secure;
3) The data is only being used for the purpose it is collected;
4) The business entity collecting such data should share the data further only to reliable data processors who have reasonable systems to comply points 1 to 3 immediately above.

With the aforesaid the submissions of MMT stand concluded

**For and on behalf of MakeMyTrip (India) Private Limited**

**(Saurabh Taneja)**
**Authorized Signatory**