Executive Summary

No sector of the global economy has been more rapidly transformed in the last five years than telecommunications. With a swiftness that has left traditional analysis and the entire system of regulatory interaction with the industry obsolete, the industry has changed its entire purpose and behaviour. Because this change has been so little reflected at the visible level of hardware infrastructure, it has passed for invisible altogether in most of the world's regulatory and legislative dialogue.

The telecommunications sector now exists to collect behavioural data on its customers. The traditional sectoral business model of selling circuit- and then packet-switched telecommunication was replaced in the early 21st century by models based first on premium content distribution and then on "over the top" data services. But with the advent of the smartphone and other mobile data devices, the "outbound" packets in the telecommunications network are just the bait on the stage of the mousetrap. The real economic value of the relationship with the customer is the "inbound" packets providing real-time surveillance of individuals' behaviour and thoughts. This data, aggregated and analysed by the new, "big" data science, is now widely characterized as "the new petroleum," the fundamental input commodity to the next phase of socio-economic development.

Learning to treat the "telecommunications sector" as the "behaviour collection and surveillance sector" is not a matter of incremental alteration in the regulatory structure. A bygone regulatory environment must be reconceived in order to deal with a completely reconfigured economy. The questions presented in this consultation reveal the depth of the disconnection between the existing regulatory framework and the new technical and economic reality.

Without simplified rules about data-collection, usage and a strict enforcement of those rules resulting in high pecuniary damages within a fixed period of time, we are merely going through the motions and will end up building yet another burdensome administrative system that will enrich lawyers while checking infringement of privacy.

TSPs should give users meaningful choice, transparency in data-collection and usage and an ability to opt-out of the octopus-like grip of data collectors as and when they choose.

All TSPs should be prohibited from making “take it or leave it” offers, meaning a TSP should not be allowed to refuse to serve a customer who does not consent to the use and sharing of their personal information for commercial purpose.

Towards this end, we recommend the following:

- The data protection framework of India should be designed in accordance with the nine National Privacy Principles laid down in the A. P. Shah Committee Report: Notice, Choice & Consent, Collection Limitation, Purpose Limitation, Access & Correction, Disclosure of Information, Security, Openness and Accountability.
- A new and independent data protection authority should be established under the aegis of the Ministry of Electronics, Information and Technology (MeitY) in order to deal with issues of data privacy and data protection in an unbiased manner. This authority should have the power to hear complaints, investigate instances of violation of data privacy, and issue directions and orders to data controllers.
- Over-the-top applications should not be subjected to telecommunications licensing requirements. However, they must abide by India’s data protection requirements under a new data protection framework.
- Users should have the ability to delete all their data from a service provider.
- Retention limitation: User data must be deleted once the purpose for collection of that data has been achieved.
- Users must be notified as soon as possible about law enforcement access to their data.
- Privacy notices should be simplified and translated into regional languages.
- There should be a requirement to ensure that anyone with whom the data has been shared is also under a legal obligation to provide a comparable standard of protection.
- Consent, although important, should not be allowed to be used by data controllers and data processors to override a consumer’s rights.

- There should be an oversight mechanism for Rule 8 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 to ensure that reasonable security measures are taken to protect data. CERT-In or a new data protection authority could be tasked with reviewing data protection audits, and investigating and prosecuting instances of data breaches and lapses in implementing reasonable security measures.
- Users should be notified about any data breach that could affect them, along with the remedial measures available to them.
- The government should set up grants and funds for projects which aim to improve the data protection and security ecosystem for all stakeholders. FOSS projects that are known to provide standards-based solutions to enable security and privacy of data should be financially supported by the government.
- Any deviation from the standard practices in a certain industry must be disclosed in clear and explicit terms by the service provider or manufacturer/seller of a product so that a user/consumer knows what to expect.
- Device manufacturers, service providers, sellers, and all other entities involved in the manufacture, sale and provision of devices and services should not be allowed to interfere with secure data transfers and secure communications in any manner.
- Compliance with the web browser based ‘Do Not Track’ standard, and a new ‘Do Not Serve Advertisements’ option, should be made compulsory for a body corporate that operates in India or targets Indians.
- All parts of the digital ecosystem, including hardware and software such as routers, IoT devices, mobile devices, laptops, desktop computers, among others and the software that runs such hardware including, but not limited to, operating systems, applications and web browsers must comply with the standard data privacy and protection norms of the country.
- The power of law enforcement agencies under Section 69(3) of the Information Technology Act, 2000 should not extend to forcing decryption of information that is infeasible for the service providers, or where the service provider has employed end-to-end encryption. Service providers should not be forced to create backdoors in their products and services.

Q.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?

No, they are insufficient to protect interests of the telecom subscribers. They are archaic, ambiguous and toothless. There is an urgent need to modernize the regulatory environment through a comprehensive privacy framework that accounts for the technical realities.

The ecosystem referred in the consultation paper is broad and it includes telecom operators, mobile apps, operating systems and ad networks among others. The measures currently applicable to all the players in this eco-system are insufficient to protect the interests of telecom subscribers. The Unified Service License Agreement and ISP License Agreements require compliance with the Information Technology Act, 2000. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("the Rules") under Section 43A of the Information Technology Act, 2000 do have certain protections for personal information and sensitive personal data however, these protections are both insufficient and unenforceable in most circumstances. A breach of these Rules can only be enforced by way of compensation to the person affected if a wrongful loss or wrongful gain can be proved. Currently, the loss or gain caused as a result of such a breach is difficult to ascertain, This should be replaced by high statutory damages to deter would-be violators. Any contravention of the Rules where wrongful loss or wrongful gain cannot be proved is punishable with a fine of up to Rs. 25,000/- under Section 45 of the IT Act. These Rules are effectively toothless in an era when European data protection regulations prescribe a fine of up to 4% of the total worldwide revenue of the erring company. Additionally, the Rules suffer from a lack of proper protections for personal data or information as they were created under a Section that was meant to provide protection to only sensitive personal data or information.

ISP License Agreements limit the encryption strength to 40 bits. Though this clause has been removed in the newer Unified Service License Agreement, the newer license continues to prohibit the use of bulk encryption equipment while still requiring service providers to ensure the privacy of subscribers.

Currently, the obligations on those who collect and process data include:

(a) Obligations on TSPs under Unified Service License Agreement or ISP License Agreements.

(b) Obligations under The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under Section 43A of the Information Technology Act, 2000.

(c) Obligation to inform CERT-in (Computer Emergency Response Team of India) about data breaches under Rule 12 of Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.

In case of a data breach, data controllers should be under an obligation to inform affected users in addition to informing CERT-in and any other regulatory bodies as may be necessary under sectoral laws, rules and regulations. Under Rule 5(4) of the Rules, retention of sensitive personal data or information is not allowed "for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force." We recommend that there should be an obligation to delete all personal data or information, not only sensitive personal data or information, once the purpose for the collection of data has been achieved. Currently, there is an obligation to delete only sensitive personal data after the purpose has been completed. This is insufficient as personal data can be used to identify, track and profile people. Deletion of all personal data must be made mandatory in order to prevent misuse of collected data.

The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 provides for a bar on automated marketing communications without consent; require identification of the communicator; require a notice of purpose of collection of data before the data is collected for marketing; allow users to determine what, if any of, their personal information exists in a directory, and to verify, correct or withdraw such data; bar processing of location data without consent unless the data is anonymized; require service providers to take appropriate measures to safeguard security of personal data; require a notice of risks of security breach and possible remedies, and a notice of any security breaches that have occurred.

However, telecom subscribers in India do not get similar protection from misuse of data. There is limited protection from unsolicited communications as outlined in the Telecom Commercial Communication Customer Preference Regulations, 2010. There is a need for a legislation to protect the privacy rights of telecom subscribers as well as users of electronic communication services in line with the law in EU.

Section 11(1)(b)(iii) of the Telecom Regulatory Authority of India Act, 1997 enables TRAI to "ensure technical compatibility and effective inter-connection between different service providers." Under this sub-section, TRAI can mandate a technical measure to ensure that service providers provide a method to port data from one service provider to another. Upon a user's request, a service provider must provide the user with all data held by the service provider about the user in machine readable and human readable format. Machine readable data would allow users to easily transfer their data from one service provider to another; this would allow competition to thrive in an industry where data is considered to be the new oil. TRAI can prescribe the formats in which such data must be provided, and can mandate that service providers implement a method to export and a method to import such data.

Q. 2 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?

Currently, Rule 2(i) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules define 'Personal information' as any information that relates to a natural person, which either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.' Often meta data about communications, which may not strictly fall under the definition of personal information can be used to gather information about a person. Hence, meta data should also get the same kind of protection as that accorded to personal data.

User's consent must be taken before sharing his/her personal data for commercial purposes. Personal data is innately private to a person. Unchecked sharing of personal data would be a violation of an individual's Fundamental Right to Privacy, enshrined under Article 21 of the Constitution of India, as recognized by the nine-judge bench of the Supreme Court of India in the case of K. S. Puttaswamy v. Union of India on 24 August 2017. It is the duty of the State to ensure that an individual's fundamental rights are adequately protected from unchecked violations by state and non-state actors. To this end, the measures that should be considered in order to empower users to own and take control of his/her personal data include:

(a) We should institute an opt-in system as opposed to an opt-out rules for data collection. Rules should be instituted that require individuals to opt in before companies or government entities can collect, use, and share their personal information Privacy notices should be simplified to the extent that a regular user should be able to understand what data will be taken, what purpose that data will serve, who it will be shared with, and who can be approached in case of a grievance. Current privacy notices are unnecessarily long and are written in legalese. Laymen do not even attempt to decipher the contents of these notices as they are long and hard to understand.

(b) User consent should be taken before transferring data to any third party. There should be a method through which the user is informed about the transfer of data and given a choice to opt out of the transfer within a reasonable amount of time before the data is shared with a third party. In case the data is shared for law enforcement purposes, the user must be informed as soon as possible. If the user is not informed about law enforcement access to their data, then the user cannot mount a proper legal defence or

(c) If the collection of some data is not necessary to provide certain services, then users must not be compelled to provide that data in order to obtain those services. The requirement under Rule 5(2)(b) of the Rules under Section 43A of the Information Technology Act read "*Body corporate or any person on its behalf shall not collect sensitive personal data or information unless the collection of the sensitive personal data or information is considered necessary for that purpose*." This requirement should be expanded to include all personal data or information, not only sensitive personal data or information. Providing your residential address, for example,

is not necessary to partake in a social network based on your true identity. Providing an address would be necessary to purchase a physical item from an e-commerce website or app.

(d) Users should have the right to revoke their consent at any point in the processing of data. If a user revokes their consent, then the data controller must delete the data of that user, unless the data controller has a legitimate reason to retain that data, such as a legal obligation or legal action, medical necessity, etc. Such exceptions need to be narrowly defined.

(e) Users should have the ability to access and make corrections in their data held by data controllers.

(f) Users should be able to transfer their data from one data controller to another if they no longer wish to continue using the services of a data controller

New capabilities that must be granted to consumers over the use of their Personal data:

(a) Ability to initiate proceedings against a data controller or data processor (an entity that processes data on the instructions of a data controller, but which does not exercise any decision making powers regarding the collection, use, retention or purpose of processing data) even if no wrongful loss or wrongful gain can be shown. Privacy has been recognized as a Fundamental Right by the Supreme Court of India in the case of *K.S. Puttaswamy & Ors v. Union of India* [W.P.(C) 494/2012]. Violation of the right to privacy as a result of the collection, use, disclosure or retention of personal data without consent, or as a result of inadequate protection of their data is a harm in itself.

(b) Consent, although important, should not be allowed to be used by data controllers and data processors to override a consumer's rights. If harm is caused to a consumer as a result of negligence on the part of the data controller or data processor, then the data controller or data processor must be held accountable regardless of whether or not consent was taken from the data subjects (individuals whose data is collected, stored, transferred, processed or used in any other manner).

(c) Consumers must be allowed to revoke their consent at any stage of data collection or data processing. When a consumer revokes consent, the data controller or data processor must delete the existing data about that consumer. Consumers must be allowed to revoke their consent in respect to all as well as selective data collection and processing activities. If revocation of

consent would lead to the deletion of some data that is necessary for providing the services, then the service provider should be allowed to stop offering those services to the consumer.

(d) Consumers must be allowed to access the data held about them by a data controller or data processor as it is their own data. Where such data is incorrect, they must be allowed to make corrections in the data that is held about them.

(e) Consumers must be allowed to transfer their data from one service provider to another at their own choice. Such data must be made available in both machine readable and human readable formats. TRAI could mandate a specific format in which the data must be made available by service providers upon consumer request in order for it to be importable for other service providers in a standardized manner. This would foster growth through competition for providing better services.

(f) Consumers should have the ability to easily delete all data held by a data controller or data processor if they no longer consent to the use or storage of that data.

(g) The procedure to initiate access to data, make corrections in data, delete all data, revoke consent, or transfer data from one service provider to another must be simple. Complicated procedures would serve as a hindrance to these tasks in the same manner as complicated privacy policies have served as a hindrance to understanding the nature of those policies.

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.

Data Controllers should be allowed to collect and process data that is necessary in order to achieve a specified purpose or to provide a specified service for a limited period of time. There should not be a restriction on using higher standards of security than any specific standard. Data controllers should be allowed to innovate through improvement of the security of their products and services. Data controllers should not be forced to weaken the security of their products or services, and they should not be forced to build back doors into their products or services. In the digital world, any backdoor or intentional security bypass can be found and exploited by undesirable actors including criminals. It is

impossible to create a weakness or a backdoor that can be used by only a limited set of people such as intelligence and law enforcement agencies.

Responsibilities of the Data Controller:

(a) Data controllers should not be allowed to collect and process data that is not mentioned in the notice of collection of processing, and which is not necessary to achieve the stated purpose of collection and processing.

(b) Data controllers must be held responsible for ensuring the security of personal and sensitive personal data. There should be an oversight mechanism for Rule 8 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 to ensure that data controllers are taking enough measures to protect the data.

(c) Data controllers must give notice of data breaches to CERT-in, sectoral regulators and affected data subjects.

(d) Data controllers must notify data subjects about what data will be collected, for what purpose, by whom, who to contact in case of grievance, what would be the effect of agreeing to or disagreeing to the collection of any data. Such notices should be simple and easy to understand, and must be available in English as well as the vernacular language of the region in which the data controller is providing their services.

(e) Data controllers must ensure that anyone with whom personal information or sensitive personal data or information is shared obeys the same standards of security and privacy as are applicable on the data controller. The transfer of data should not be allowed without explicit consent from the data subject. Transfer of data must not be allowed to another country unless the country to which the data is being transferred offers similar levels of protection to personal and sensitive personal data.

(f) Personal data must not be published openly. Any exceptions such as for journalism must be narrowly defined. Broad exceptions would serve as a source of exploitation.

(g) Any collection, use, storage or transfer of personal data must not be done without prior explicit informed consent from the data subject.

(h) Data controllers must be transparent about their security procedures and practices, and data collection, use and transfer policies and these should be published in the form of a privacy policy.

(i) Data controllers must train their staff in security procedures.

(j) Data controllers must ensure that access to personal and sensitive personal data is restricted to only those people who must necessarily have access to it in order to perform their duties. In all other instances, such data must be out of reach for employees and outsiders.

As data controllers are in the position to make all decisions related to collection and processing of data, only in certain specific and clearly defined situations the rights of a data controller can supersede the rights of an individual over his/her personal data. The data controller can retain data if the retention of data is necessary to comply with a law, a lawful order, a legal obligation, or for a legal action. They can also retain the data if that data is a part of the public domain. Users cannot compel a data controller to delete or stop processing anonymized data. If the deletion of some data would make it impossible for a data controller to provide a service or a product to a user, then the data controller must not be compelled to provide that service or product to the user.

An independent authority is required to regulate data controllers. This authority can be a new body along the lines of data protection authorities in Europe and other parts of the world. TRAI has the power to regulate telecommunication service providers, but not all data controllers are telecommunication service providers. We recommend that all data controllers should be regulated by a new and independent data protection authority under a new legislation focused on the issue of data privacy and protection. Such a regulator should have the power to hear complaints against data controllers, investigate instances of data breaches, and issue directions and orders to data controllers. Since India already has a body dealing with security of data in the form of CERT-In, the powers of CERT-In to regulate and decide upon issues of data security could be expanded, and a new body could be established to deal with issues of data privacy. CERT-In was established through *The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013* passed under Section 70B of *The Information Technology Act, 2000*. Section

70B(4) and Rules 8 and 9 of the 2013 Rules deal with the responsibilities and services of CERT-In. The responsibilities under Section 70B(4) include:

- collection, analysis and dissemination of information on cyber incidents;
- forecast and alerts of cyber security incidents;
- emergency measures for handling cyber security incidents;
- coordination of cyber incidents response activities;
- issue guidelines, advisories, vulnerability notes and white-papers relating to information security practices, procedures, preventation, response and reporting of cyber incidents;

CERT-In's services under Rule 9 of the 2013 rules include:

- response to cyber security incidents;
- prediction and prevention of cyber security incidents;
- analysis and forensics of cyber security incidents;
- information security assurance and audits;
- awareness and technology exposition in the area of cyber security;
- training or upgrade of technical know-how for certain entities;
- scanning of cyber space with respect to cyber security vulnerabilities, breaches and malicious activities.

Through a change in the law, CERT-In may be granted the additional responsibilities of:

- investigating and prosecuting failure to:
  - implement reasonable security procedures;
  - inform affected users about data breaches, how the breach affects them and what remedies are available to the users;
  - disclose to CERT-In and to the public at large about security procedures followed by a body corporate;
  - train staff about security procedures;
  - report instances of security breaches to CERT-In.
- interfacing with a dedicated data security officer in body corporates of a certain size – for example, body corporates with 200 employees or revenue exceeding 10 crores Rupees;
- reviewing security audits of body corporates.

Q. 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?

Technology based architectures do not operate in isolation without active application of mind through human intervention. Algorithmic biases are well-known in the industry. Harm cannot be prevented in a fool-proof manner, but the majority of it can be avoided through the use of audits as they would lead to higher compliance with data protection requirements than unchecked haphazard implementations. Other jurisdictions in the world have audit mechanisms to prevent abuse of data. Audits could be conducted to ensure that:

- data is not being collected without consent;
- notices are simplified and easy to understand;
- notices sufficiently inform data subjects about what data will be collected, how it will be used, who it will be shared with and how to raise a complaint;
- the method of collecting consent is sufficient;
- security procedures and practices match or exceed the industry standards;
- data has not been transferred to another body without prior user consent;
- data controllers conduct training of their staff in security procedures and practices.

A technology enabled architecture would enable the government or its designated authority to receive data from auditors in a standard format with the ability to easily look for errants. These audits could help in preventing future security breaches and unintended violations of privacy. The audits would act as a deterrent in selling personal data without proper consent. Data transfers for a price would appear on the balance sheets of the body corporate, but the audits cannot prevent abuse of data in the form of data transfers where a body corporate is determined to bypass the law.

The industry and industry associations could come together to train auditors to meet the requirements. Once there is a demand, a sufficiently large talent pool of auditors could be developed.

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?

To ensure innovation and creation of new businesses, there should be certainty with respect to the legal framework related to data protection. The law should be in tune with the principles of privacy followed in jurisdictions like the EU so that there is no hindrance to cross-border transfer of data, while at the same time protecting the interest of Indian users.

Currently, the quantum of fine for non-compliance with data protection requirements under the Information Technology Act and *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011* is too low. Since these Rules do not explicitly mention any punishment or fine, the only provisions under which they can be enforced are Sections 43A and 45 of the Information Technology Act, 2000. Section 43A, under which these rules were drafted, allows for compensation to be paid to a person affected by non-compliance of these Rules. Section 45 prescribes the fine for non-compliance with any provision of the Act or Rules made under it when no separate provision has been made for punishment for such non-compliance. The penalty payable under Section 45 is up to Rs. 25,000/-. In an era when data-based global technological companies are some of the richest companies in the world, with global revenue higher than the GDP of many countries, a fine of this magnitude is not a deterrent from the perspective of such companies. If it would be cheaper to pay a fine than to fix a problem, then a body corporate would choose to pay a fine instead of fixing the problem. The quantum of fine must be tied to the local or global revenue of a body corporate in order for the fine to be a deterrent.

A measure that, for example, requires encryption of a particular form for the security of data could in future be a hindrance towards the very security that it set out to protect. Vulnerabilities are regularly found in software and hardware. To ensure that data is protected from these vulnerabilities, more secure technologies have to be deployed by data controllers and data processors. The vulnerability known as KRACKs[1] (Key Reinstallation Attacks) has demonstrated that even the most prevalent and seemingly secure standards can one day become vulnerable to attack. To protect against such vulnerabilities, the

1 https://www.krackattacks.com/

legal requirement should be to implement a reasonable standard of security, along with audits of those security measures, instead of prescribing a base standard for security. A base standard for security poses a secondary problem as well – body corporates can follow the minimum level that has been prescribed and not improve upon it because it provides them with legal protection for the lowest financial cost.

The laws and regulations created to preserve the privacy and security of data must be carefully drafted to ensure that they do not encroach upon the ability to innovate by being excessively restrictive. Technology evolves faster than laws and regulations. There is a need for a principle-based approach to ensure data privacy and data security. We recommend following the nine principles outlined by the A.P. Shah Committee as the National Privacy Principles, in order to ensure that the law meets the needs of privacy and security in an appropriate manner. These principles are: Notice, Choice & Consent, Collection Limitation, Purpose Limitation, Access & Correction, Disclosure of Information, Security, Openness and Accountability.

Q.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?

The Government could use anonymized data sets for projects that are in the interest of public, for example to get health trends. With increasing emphasis on Open data, more and more Government departments and agencies are publishing data related to their area of work. At the same time, care should be taken to ensure that anonymized data is not processed to reveal identity information. Research has shown that with the help of big data analytics it is possible, and often very easy, to identify individuals from anonymized data. Researchers from the University of Texas, used anonymized data set released by Netflix and showed that it is possible to re-identify a Netflix user from the data set.[2]

2 Narayanan, A. and Shmatikov, V, Robust De-anonymization of Large Sparse Datasets, available at https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf , last accessed on Nov.7, 2017.

Research has shown that the belief that anonymized data protects privacy of users is a myth. It has been shown that anonymized data can be easily *de-anonymised* enabling identification of individuals.[3]Hence it will be ideal for Governments or authorised authority to no get into the business of creating anonymized data sets for commercial uses.

In the proposed law on Data Protection in UK, re-identifying de-identified data is an offence. [4] Measures like this could be necessary to ensure that big data analytics would not result in violation of privacy rights of citizens.

Q. 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?

The approach should be to have principles, standards and guidelines in place that would ensure compliance of service providers with the data protection regulation. Technologies could change at a fast pace making any solution designed obsolete in no time. However, standards and guidelines could ensure that irrespective of technologies, the goal of protection of privacy rights of citizens is taken care of. It is important to have a data protection authority that would ensure compliance of service providers with standards and guidelines that would help to protect the privacy rights of users.

Q. 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?

- It is important to adopt Free and Open Source Software (FOSS) which are auditable over proprietary software which are closed and are not auditable.

3 Ohm, Paul, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (August 13, 2009). UCLA Law Review, Vol. 57, p. 1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12. Available at SSRN: https://ssrn.com/abstract=1450006

4 https://publications.parliament.uk/pa/bills/lbill/2017-2019/0066/18066.pdf ,last accessed on Nov.7, 2017

- Support FOSS projects that are known to provide standards-based solutions to enable security and privacy of data. These projects could be standalone tools or libraries (modules, addons) used in other developing software.
- Set up grants and funds for projects which aim to improve the data protection and security ecosystem for all stakeholders.
- Announce incentives (cash prizes, scholarships, recognitions) for individuals or organizations who follow responsible disclosure of security flaws in technologies that handle sensitive personal data.

As the Equifax breach has shown us, it is important to have proper Information Security practices. It is imperative to have an organisational culture that places emphasis on security.

Q. 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?

TRAI has no jurisdiction to control these players as all policy matters relating to information technology, electronics and Internet (except licensing of ISP) fall under the domain of MeitY, not TRAI.

Key issues of data protection pertaining to the collection and use of data by various stakeholders in the digital ecosystem, including content and application service providers, device manufacturers, operating systems, browsers, etc:

(a) If a product such as a device or an operating system is being sold, then users must be provided a way to access and accept or reject the privacy policy of the product before paying for the product.

(b) Operating systems and device manufacturers have disproportionate power of holding their users hostage to giving up their data or being unable to use a product that they've paid for.

(c) Browsers act as gatekeepers to the internet. While operating systems and device manufacturers have the ability to capture everything that anyone does on the device, browsers have the ability to capture all data related to a person's online activities.

(d) Various companies such as those in the online advertising business make use of cookie based trackers and fingerprinting mechanisms to gather user data and to profile users.

(e) All stakeholders in the digital ecosystem, including those mentioned above, have the ability to collect, use and/or transfer data for which they did not collect explicit consent.

(f) Any data is only as secure as the weakest link in the chain. As such, it is necessary to ensure that all parts of the digital ecosystem abide by data privacy and data protection norms.

Mechanisms that need to be put in place in order to address these issues:

(a) Any deviation from the standard practices in a certain industry must be disclosed in clear and explicit terms by the service provider or manufacturer/seller of a product so that a user/consumer knows what to expect. If such deviations would intrude upon the privacy of a user, the company should be obligated to clearly disclose and highlight what the impact of such a deviation from the norm would be on the privacy of the individuals using that service or product.

(b) Device manufacturers, service providers, sellers, and all other entities involved in the manufacture, sale and provision of devices and services should not be allowed to interfere with secure data transfers and secure communications in any manner. For example, Lenovo installed a malware called Superfish in its Windows based laptops.[5] This malware intercepted all secure communications taking place in web browsers by replacing their security certificate by a self-signed certificate from the malware itself. This weakened user security by preventing them from knowing when they were visiting a website that had a spoofed certificate, and compromised their privacy by intercepting secure communications with their banking, shopping and email websites, among others.

5 https://www.theregister.co.uk/2015/02/19/superfish_lenovo_spyware/

(c) Consent should be explicit and clear. A system of opting out of consent must not be allowed to take free reign wherever privacy and security are concerned. For example, when Microsoft allowed a free upgrade to Windows 10 for users of Windows 7 and Windows 8, it employed a deceptive tactic to get users' consent.[6] The act of closing a window is commonly an action to dismiss something without accepting it. The upgrade software considered the act of closing a window to be acceptance of the option to upgrade to Windows 10. The upgrade to Windows 10 had various implications on the privacy and security of end users as Windows 10 sends their data to Microsoft's servers for analysis and user profiling, among other things.

(d) Browsers must not be allowed to:

a) transfer browsing history, cookies, cache data and form data from the local device for any purpose other than syncing across user devices;

b) interfere with security of data transfer by replacing security certificates;

(e) A web browser standard called 'Do Not Track' exists to assist users in easily signalling to websites that they do not wish to be tracked. Compliance with this standard is currently not compulsory. The majority of websites ignore this signal and continue to track users despite their clear expression that they do not wish for such tracking and profiling to take place. Users should have the ability to easily block all web based trackers and advertisements to protect their privacy. Ad-blocking could take the form of an option in web browsers, similar to the Do Not Track option, that signals to websites that a user does not wish to be served advertisements. Compliance with both of these signals: Do Not Track and the new Do Not Serve Advertisements, should be made compulsory for a body corporate that operates in India or targets Indians.

(f) All parts of the digital ecosystem, including hardware and software such as routers, IoT devices, mobile devices, laptops, desktop computers, among others and the software that runs such hardware including, but not limited to, operating systems, applications and web browsers must comply with the standard data privacy and protection norms of the country. Without these norms being applicable to all the players in the ecosystem, loopholes would be left behind for data to be gathered and exploited. Towards this end, the National Privacy Principles recommended by the A. P. Shah Committee can serve as a good guideline for the norms that

6 https://www.pcworld.com/article/3014238/windows/get-windows-10-prompt-adopts-malware-like-tactics-to-trick-you-into-upgrading.html

should be followed by all the stakeholders. These include: Notice, Choice & Consent, Collection Limitation, Purpose Limitation, Access & Correction, Disclosure of Information, Security, Openness and Accountability. These principles are being followed in data protection laws in most parts of the world, with new countries constantly joining the fold of those that have laws that allow personal data to be shared with recipients in only those countries that also have similar protections in place.

Q. 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?

The data protection norms applicable to TSPs are mainly contained in the IT Act, Telegraph Act and various license agreements.

1) Telegraph Act:

- Section 26 makes it an offence for a Telegraph Officer to alter, unlawfully disclose or acquaint himself with the content of any message.
- Section 30 criminalizes the fraudulent retention or wilful detention of a message which is intended for someone else.

Section 43A of the IT Act (Compensation for failure to protect data) and Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules 2011 formed under section 43A of Act define a data protection framework for the processing of digital data by body corporates.

TRAI established the Telecom Unsolicited Commercial Communications Regulations, 2007 in an attempt to prevent Unsolicited Commercial Calls to telecom consumers. A National Do Not Call Register was established under it, which contains information regarding consumers who do not wish to receive unsolicited commercial communications. The regulation also specifies the procedure for

initiation of complaints by consumers and for their adjudication and disposal. It also imposes fines on telemarketers who initiate UCC with individuals who have opted not to receive such communications. It also provides for every access provider and the person authorized to maintain the National Do Not Call Register and to keep confidential all the information disclosed by the subscriber and entered in the National Do Not Call Register.

Similarly, the Telecom Commercial Communications Customer Preference Regulations, 2010 provides for setting up a Provider Customer Preference Register/ National customer Preference Register/ National Telemarketer Register. It contains provisions for maintaining privacy and protecting customer information.

On 26th February 2010, TRAI issued a direction to make sure that the compliance of the terms and conditions of the licenses regarding confidentiality of information of subscribers and privacy of communications were carried out.

TRAI directed Cellular Mobile Telephone Service Providers and Unified Access Service Providers:[7]

- To ensure confidentiality of information as provided in the license conditions;
- To put in place appropriate mechanisms so as to prevent the breach of confidentiality of information of the subscriber and privacy of communication; and
- To furnish to the Authority, within fifteen days of issuance of this Direction, the details of steps taken by the service provider to safeguard the confidentiality of information of subscribers and privacy of communications.

The detailed guidelines regulating the behaviour of TSPs are contained in the terms of the licences issued, which permit them to conduct business, frequently, these licences contain clauses requiring TSPs to safeguard the privacy of their consumers.

7 http://www.trai.gov.in/sites/default/files/Directions-26-Feb-10.pdf

Apart from the aforementioned regulations, National Long distance license, ISP license categories (A, B and C) and Unified service license issued by the Department of Telecommunications (DoT) contain provisions specifying a certain degree of data protection.

Further, the Telecom Engineering Centre specifies common standards regarding telecom network equipment, services, interoperability, generic and interface requirements, among other things.

Since OTT applications are unlicensed, they do not have to comply with TRAI and DOT regulations. They however have to abide by the provisions of the IT Act and the complementing Rules.
Although, OTT applications should not be subjected to licensing as it will hamper innovation, they should abide by the proposed data protection law and regulations. There should be greater parity in the data protection norms applicable to TSPs and other communications service providers offering comparable services. A comprehensive data protection framework to protect user data from misuse is the need of the hour.

Q. 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?

Legitimate exceptions should be limited and narrowly defined to avoid abuse. These should include:

- Section 69(3) of IT Act allows for a lawful order to intercept, monitor or decrypt some information. This should not extend to forcing decryption of information that is infeasible for the service providers, or where the service provider has employed end-to-end encryption. Forcing a service provider to create a backdoor in an end-to-end encryption system would weaken the security of all users of that service provider. Such a damage to the security of all users is disproportionate and must not be allowed as a fallout of an attempt to access the messages of a few.

- Service providers should be allowed to retain data that is necessary for the performance of a legal obligation or a legal procedure. However, this exception should be defined in such a way that it cannot be used by law enforcement to force service providers to collect any data that the service provider would not have otherwise collected from the user.
- Data that has been fully anonymized with no way to link it back to any person should be allowed to be used and shared in any manner by the service provider. If the data is only partially anonymized, then data protection requirements should continue to be imposed on that data in order to minimize the chances of privacy violations.
- Data should be allowed to be used for medical research and other research that would result in societal advancements after the data has been anonymized as far as may be feasible.
- Data that is available in the public domain does not need to fall within the scope of data protection requirements.
- Freedom of press should be upheld by allowing press to publish information that is in the interest of society. This exception should not allow the press to publish sensitive personal information such as biometric data.
- Data subjects should be informed about law enforcement access immediately after the access to their data. Where such a notice would jeopardize the safety or security of the state or investigation or prevention of an offence, the data subject should be informed as soon as such a danger has passed. A data subject cannot defend his/her legal rights if they are not made aware of violations of those rights.

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?

Companies should not be allowed to transfer personal data out of India unless the country to which that data is transferred has the same level of protections available. Without such a clause, data could be transferred out of India to another country with fewer protections and more freedom to violate data privacy. Under the European General Data Protection Regulation, transfer of personal data for

processing to a third country or international organization outside the EU can be done by the means of an adequacy decision, i.e. if the Commission decides that the third party ensures an adequate level of protection. 'Adequacy' is decided by analysing the rule of law, legislations in force, defence, national security, effective functioning of independent supervisory authorities responsible for data protection, among other things. Without an adequacy decision, a controller or processor can direct such transfer after ensuring that there are appropriate safeguards in place by means of binding corporate rules or standard data protection clauses as adopted by the Commission or a Supervisory Authority. Both of the above methods can be disregarded if for example, the data subject has consented to the transfer, after being given due counselling of the risks, or if it is necessary for fulfilling compelling public interest or performance of a contract between the data subject and the controller. Similar laws exist in multiple countries.

The issue of jurisdiction is challenging in the digital sphere, but here too, the GDPR has made great strides. These can be appropriately modified and implemented in the Indian legal system. If the website or service targets Indians, then it must obey Indian laws and regulations. In order to determine whether it a website or a service targets Indians, the following things could be checked:

- It uses an Indian language; or
- It allows people to enter an Indian address; or
- It mentions India, Bharat or Hindustan prominently; or
- It allows payments to be made in Indian rupees; or
- It has a registered office located in India.

Jurisdiction can be enforced by:

- Local agents of a body corporate that is located outside the country can be held liable for the actions of the body corporate. Local agents could include employees of the body corporate, local office of the body corporate or a subsidiary of the body corporate.
- Each body corporate that targets Indians may be required to have a data protection officer located in India if the body corporate is of a certain size, for example, if the body corporate has 200 employees or a revenue exceeding 10 crore Rupees, there could be a requirement to have a

local agent in India that is held responsible for the actions of the body corporate. Please note that these figures are for representational purposes only.

- A website or a service that targets Indians but does not obey Indian laws / regulations and against which there is no way to enforce Indian laws and regulations may be prevented from operating in India or targeting Indian users.