TRA
Lawyers for innovation

Tabular Mapping Of Stakeholders' Responses to Question 2 – TRAI Consultation Paper: Definition of Personal Data, Consent and Empowerment of User

---

The following table was prepared after analysis of responses of all fifty three (53) stakeholders to Question 2 of the Consultation Paper, *"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 table identifies the stances of the stakeholders and their response to the question. It also states the suggestions they have made to the TRAI in view of the question posed. As mentioned earlier, the responses of the stakeholders have been categorised in a manner that corresponds with some of the issues raised in Part II and Part III the White Paper, namely, the definition of personal data and consent as the ground for sharing of personal data.

Sl. No.	Stakeholder	Definition of Personal Data	Permissible Grounds and Measures for Processing Personal Data	User Empowerment Measures/New Capabilities for Consumers	Other Comments
1.	Internet & Mobile Association of India (IAMAI)	The definition is in line with international norms. Definition must be inclusive and non restrictive and must allow for future developments in technology.	Rights and consent based approach recommended. Consent is needed for sensitive data but not for non-sensitive data. It should be clearly defined where consent is needed. There might be instances of consent fatigue. Consent should not be in isolation but in combination with transparency, access and prevention of harm. Entities should ensure that data protection is proportionate to purpose, abide by transparency.	There should be consumer awareness programmes.	Processing of anonymised data should be incentivised. Singapore and Japan provide a good referral point when it comes to processing of anonymised data. Market driven developments that lead to increase in user transparency should be recognised by law.

2.	Association Of Competitive Telecom Operators (ACTO)	Definition of personal data is in lines with international norms. Definition should not be broad and ambiguous. The definition of personal data should not include information that has no immediate connection to a specific individual Any new data protection framework should allow for the use of de-identified data and aggregate data.	TRAI should take into consideration Singapore's Review of Personal Data Protection Act in Indian Context. "Notification of purpose" requirement has been proposed by the Singapore Personal Data Protection Commission as per the Public Consultation for Approaches for Managing Personal Data in the Digital Economy relying only on consent for the collection, use and disclosure of personal data may have deleterious effects. An approach that calibrates the balance of responsibilities and adopt pre-emptive preventive measures can meaningfully address the consent requirements.	__	Legal framework should rely on strong principles and business-level accountability to avoid over-expansive and inflexible regulations.
3.	Associated Chambers of Commerce and Industry of India (ASSOCHAM)	No need to modify the definition of personal data. A foreign approach would be ill suited to Indian setting.	Consent is one potential ground but should not be the only valid ground on which data may be collected or processed. Users must be given the choice of	__	Data protection legislation must be guided by the priorities of enabling

			providing implicit consent or permitting processing on other legitimate grounds. (example, GDPR – "lawful processing") This especially becomes important in cases where entities have to protect valid security or other interests and receiving consent is impractical.		innovation, the ease of doing business, preserving the diverse character of the internet while at the same time ensuring that privacy interests of citizens are satisfied.
4.	Cellular Operators Association of India (COAI)	There is no need for any amendments in the definitions. Difference between "Personal Information" or "Personally Identifiable Information" project (PII) and anonymized or aggregate data should be acknowledged.	User's consent should be needed only if the user's data is being shared in any user identifiable format. No consent needed for sharing of anonymized data, except that the privacy policy will mention the recipient and purpose of sharing/use of such data.	There should be facilitation provided to deletion of personal data except that which is needed to be stored by law.	__
5.	Groupe Speciale Mobile Association (GSMA)	No changes are required in the definition of personal information. It is quite broad and hence does not require any changes.	Pseudonymization of data can provide safeguard without consent. Consent fatigue is a problem that consumers face. There should be other flexible	__	International transfer of data should be there only if the country has an adequate

		Reasonable Security Practices Rules should make a clear distinction between the principles that apply to processing of all personal information and those additional protections that apply only to processing of Sensitive personal data or information.	grounds for the purposes of processing of data in order to maximise chances of innovation. Processing should be done for purposes that are compatible with the original purposes, or processing where it is in their legitimate interests to do so and the interests of the individual do not outweigh those of the company. There should be tools to "opt in" or "opt out" of certain processing and by providing easy access to the data and their previous consents. Consumers should have the right to be forgotten. On termination of services the request to terminate his/her data must be considered.		level of protection. In specific cases, international transfer of data may have an impact on national security and this should be assessed on a case by case basis. Further, a number of tools have been developed in other jurisdictions to help organisations manage data flows, such as the APEC cross-border privacy rules, the EU Standard Contractual Clauses. Entities who transfer personal data (either sensitive or less sensitive data) to other countries

					should be subjected to the privacy and data protection laws of the country where the services are being provided to the customer.
6.	Internet Service Providers Association of India (ISPAI)	No need of changes in definition.	Explicit consent is mandatory for the personal information whereas it would not be required in case of non-personal and aggregate information. This distinction will help in development of innovative services & help the organization to make use of big-data analytics. The pseudonymisation of personal data can provide better way to protect the data while usage without the need for explicit consent of the customer.	The entities should be made liable for any negligence with privacy and protection of personal data according to the rules of the country in which the services are being offered. The entities should also adhere to the customer's right to be forgotten (when they stop the services) and help the customer to gain access to sharing his personal data by providing a technology	__

				based solution to manage their "opt-in" or "opt-out" consents. On termination of services data must not be allowed to be stored other than which is required by law.	
7.	NLUD	As mentioned in the Consultation Paper, in addition to identifying information that typically falls within the definition of personal information, telecom companies collect and have access to specific types of information about their subscribers such as call detail records, calling patterns, location data, data usage information. Data protection rules applicable to these companies need to account for this and protect consumers from the privacy	It is our recommendation that additional accountability and transparency mechanisms should be implemented to help users retain more control over their data. The European Standards mentioned above include examples of some such measures. An indicative list of measures that may be adopted to provide users with additional control over their data is provided below (i) Opt-in and opt-out mechanisms, including complete or partial opt-out or withdrawal of consent	The following measures must be taken (ii) Data breach notification requirements (iii) Accessible redressal and dispute resolution mechanisms (iv) Right to access, review and correct data. (v) Right to data portability.	Regular privacy impact assessments and audits will help increase users' trust in data collectors and processors, and allow for more meaningful implementation of the above-mentioned Principles / measures Three main principles of data

		violations that result from these practices. The European Union's new GDPR provides one example of the sort of wide definition that is necessary in this context, 'personal data' is simply defined as any information relating to an identified or identifiable natural person. The definition goes on to provide that an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. While most of the data protection regulations in the GDPR apply in relation to all such personal information, additional safeguards are applicable to in relation to			due process are proposed (i) Notice (ii) Opportunity for a hearing (iii) Impartial Adjudicator and Judicial Review

		special categories of data. We recommend the adoption of this approach.			
8.	Span Technologies	__	Not answered this question directly, but only in context of Aadhaar. For Aadhaar to be privacy compliant, it must intimate the user when any of his personal information is sought, purpose of its collection and usage and it will be shared with any third parties. Thereafter, the user should have the choice to opt-in/opt-out. There should be limitation for the purpose it is sought. User should have access to his data so that he could amend the same. Aadhaar's management needs to be made accountable to an independent, autonomous auditing authority (more on it stated later) for ensuring compliance with privacy requirements as per law which investigates breaches of privacy based on complaints by users.	__	It should be defined to what extent individuals can exercise control over their data. User's privacy should not be compromised. Privacy rights needs to fully address individual's autonomy and consent in a manner such that it safeguards against unlawful surveillance. As stated by The State should strike the delicate balance between safeguarding national security

			There should be multi factor authentication in a manner such that it addresses three main factors something you are (based on biometric), something you have (based on voter ID/driving license) and something you know (based on pattern, pin or password).		and Sovereign interest and ensuring that individual privacy is not imperilled.
9.	TRA	_	__	__	__
10.	National Association of Software and Services Companies (NASSCOM) – Data Security Council of India (DSCI)	The proposed legislation and/ or subsequent guidelines/ rules and case laws should try and recognize the role that purpose, context and proportionality play determining whether a particular piece of information in isolation or in combination with other information constitutes personal information in that specific context, beyond the general rule. PI could also addressed by sectoral regulators. As the	Combining consent with other factors helps. Under EU GDPR Consent principle, consent should be informed, unambiguous, freely given, requires affirmative action (silence or non-action should not be deemed as consent), should not be mixed with T&C, must be demonstrable, revocable etc. The consent should not be considered as simply responsibility/liability transferring tool but should be	User empowerment can cover various aspects which include efforts by government, regulator, organizations, educational institutes and others. Sensitization on the perils of a privacy breach for individuals/data	__

		regulation should strive to be technology neutral, the PI definition should be formulated keeping in mind various other aspects and nature of data such as purpose, collection, consent, access, proportionality with sensitivity, individual identifiability, etc.	practiced along with other privacy principles to provide desired respect to individuals' privacy. The data protection regime in India too may identify the set of PI which requires explicit consent and other specific requirements but also consider the reasonability of executing it by the organizations. Other factors which can define the meaning and serve the purpose of taking consent may be, but not limited to, sensitivity of data, time when it is taken, language used, notice provided, audience and repercussions of giving such consent. The consent should not be considered as simply responsibility/liability transferring tool but should be practiced along with other privacy principles to provide desired respect to individuals' privacy.	subjects as well as organizations collecting and processing PI for business use is essential. Empowering users with privacy principles and adequate rights to control their personal data would be limited if users would not be aware of it or would not know the way of exercising the same. Awareness campaigns must be conducted and organizations must be obligated to impart individuals with an understanding of how they may ay exercise their privacy rights. In order to give better control over their personal data to individuals the	

				following may be considered · Access and rights to edit and rectify personal information - Both information collected directly from individual, as well as developed by the organization basis monitoring the individual and has the potential to identify the individual in isolation. · Data should be adequately anonymized and not include individuals' behavior, trend, digital/online profile, preferences, etc. which may breach individual's privacy. · Data Portability and Right to be Forgotten/Erasure are	

				two specific rights that have been explicitly crafted in EU GDPR (European Union General Data Protection Regulation) for giving more control to the users over their personal data.In India there is an evolved expectation of right to privacy to end users. Other innovative ways maybe evaluated by the businesses to award more control to individuals over their personal data.	
11.	Association for Competitive Technology (ACT)	__	It is important to calibrate enforcement mechanisms to the risk involved, and the actual harm to the consumer, instead of basing it exclusively on one principle of consent. Hence	__	__

			consent should not be the only basis.		
12.	Zeotap India Pvt. Ltd.	Anonymized data that cannot be used to identify and locate/profile/track any individual must be kept outside of the ambit of personal data definition. To explain further, exceptions could be carved out for identifiers that identify a device, not individual and are non-persistent, examples being cookie or Ad ID (resettable, or can be purged from the equipment). Anonymized and Pseudonymized data does not infringe on the right of privacy of any subscriber and hence may be allowed to be used for provisioning of new innovative services.	Non sensitive data should require only implied consent. Hence, different kinds of data should be treated differently.	The subscriber should be informed about available opt-out option to enable him/her to opt out at any moment of time.	__
13.	Takshashila Institution	The definition of personal data must be expanded. The definition of personal data should not only cover information that allows easy	A new data protection framework must focus on certain inherent rights that people have over their data. Even if user consent is sought for certain	__	__

		identification of a natural person, it should also encompass anonymised aggregate data which can become personal information through the addition of one or more filters.	services, they should not be designed as "take it or leave it" clauses. The user should have the ability to view the granular aspects of his consent, so that even if he does not agree to providing some data, he should be able to avail of the services of the data controller to the extent applicable.		
14.	Information Systems Audit and Control Association (ISACA)	__	Data should only be used for the purpose that it was collected for If a data controller wants to use the data for other purposes consent should be obtained from data controller.	Individuals should be able to know whether or not personal data concerning them is being processed, where it is being processed, and for what purpose. The following rights must be available to the consumers. Right to information TSPs must inform individuals about all information that is collected and also	__

				information that is being derived from their data. Right to forget Individuals must be afforded the right to be forgotten. Data portability —the data protections afforded to India's citizens travels with them, regardless of where in the world their travels take them.	
15.	IBM	Identifiability may not be a meaningful differentiator to determine what should and should not be covered by Data protection rules. Hence, there is need for some amendment.	Once a user has opted out of the service the data controller must not be allowed to use the data already collected. Consent should be in the language of the user and/or in the language of choice.	There must be right to data portability. The right to Data portability will require businesses to ensure that they hand over the personal data provided by an individual in a usable and transferable format to the	__

				regulator/Government or to a third party.	
16.	Make My Trip	The definition is sufficient in the current scenario.The extent and purpose of definitions (under the Personal Pata Protection Bill, 2014 and the IT Rules, 2011) is sufficient in the current scenario.	Consent should be taken before sharing of personal data. It has to be clarified what is “commercial purpose”. "Commercial purpose" can mean usage of individual's data for purposes other than this transaction for which the individual has shared his data. Repeated requests for consent is an onerous obligation. 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.	__	__

17.	Access Now	There must be certain amendments. use of the term 'User' in place of 'Consumer' as a user may not be a subscriber of a particular SP, but his data may still be implicated. Further, a user must include a current or former, paying or non-paying subscriber as well as an applicant for the service. With respect to telecommunication data, a TSP acquires in connection to its provision of telecommunication services, the following kinds of data Any information that is linked or linkable to the user. Must include 1. Time and location of communication that it originated from; 2. Information about device that sent or made the communication; 3. Recipient of the communication and their	Any use of data by SP, except for the purpose of providing / marketing the telecommunication service, must be based on consent of the user. 'Opt-in' is preferred in place of 'opt-out'. Opt-in must be affirmative, express, and adequately informed, and must require explicit consent specific to the data and the purposes. Opt-out mechanisms typically suffer from cumbersome processes, offer little notice or explanation on the nature of the use, and often even deliberately hide the methods and purposes of corporate programs that track users.	There must be all possible opportunities for notice and remedy. The costs to providers in the digital age should lower as more users take advantage of 'paperless' delivery options and electronic delivery becomes the norm. Every user should be able to access their data by simple request.The information should be provided to the consumer in electronic form or paper based on the consumer preference and free of charge. There should be a remedy if information is not provided. Consumers should further have a right to correct their information if	__

		location and device, and time received; 4. Length of a communication or the size of a message; 5. Location during social media updates, application updates or any similar automated 6. checks on connected smartphones Information arising out of User's use of the service - 1. That relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service, made available to the SP solely by virtue of customer-service provider relationship; 2. Information contained in bills; 3. Other categories of data which need to be protected geolocation, device identifier data, destination of web traffic as tracked by domain names and URLs, traffic data, port,		inaccurate or out of date. Beyond access and correction, consumers control over their information should extend to the ability to object, to erasure, and to data portability. The ability to object enables consumers to refuse the collection and use of specific types of information.	

		application header, application usage; 4. Any definition of data should be technology neutral and broad, We recommend that both types of information be protected.			
18.	U.S. India Strategic Partnership Forum (USISPF)	The Indian definition is broad enough to cover changes due to technological advancements. It should however, be applied proportionally. Proportionality means that the appropriate level of protection is applied to different kinds of information.	Consent should free, and without undue influence or misrepresentation. Too many consent-related privacy choices and requests to collect data should not be mandated. Therefore, it is important to let companies use "legitimate interest" as a legal ground for data processing. This is a valid ground in many jurisdictions, and enables companies to collect data that is necessary to support, deliver and improve a variety of services for the benefit of users, data controllers or the society. There should be a flexible approach to consent. Beyond a basic set of controls, it should be	Given that privacy means different things to different users, it is important to put users in control by providing the necessary information and options to exercise their choice meaningfully wherever relevant. For instance, the Android OS platform empowers users to grant granular permissions to the apps they install on their devices through the Play store.	__-

			left to the company in an agreement with the customer to determine the appropriate terms for consent. Company should adhere to its own policy in the case of enforcement.	Through easy to navigate settings, users can change these permissions anytime. To enhance user transparency and trust, many companies provide 'one stop shop' privacy help center, easy to understand privacy notices, single view of what PI is collected and processed by the Company. Additionally, some companies are empowering users by providing data portability, allowing users to download their data from the platforms they use, even potentially moving their data to competing platforms.	

				Data portability and interoperability help users avoid feeling locked into any service, and give them the freedom to seek the products that work best for them. The law should recognize these market/industry driven developments that have led to increase in user transparency and trust.	
19.	Information Technology Industry Council (ITI)	Identifiability may no longer determine the scope of data protection rules. Hence, a concept of risk should be built into the data protection regime, measuring the likelihood of concrete harm to individuals if their personal data is transmitted or disclosed, and thus preventing an overbroad	For consent to be effective it should be sensitive to context. Methods and techniques of requesting consent should evolve.	There should be data portability.	__

		application of data protection obligations.			
20.	Sigfox	Beyond technology innovation, universal definition of personal data in non-obvious context (e.g. identifiers, names, etc.) will more often depend on specific cases and therefore require a flexible approach. Such a approach would require all stakeholders and consumers to be empowered to negotiate the right level of data control and liability between each other.	There should be development of technology neutral regulation These regulations should focus on desired privacy outcomes, rather than specifying technological means to direct privacy practices. With this regard, when mechanisms such as systematic anonymization or privacy-by-design principles are implemented to guarantee the right level of data privacy and appropriate information are provided to end-users, it should be made possible to avoid user's consent before sharing the data for valuation purposes.	__	__
21.	Exotel Techcom Pvt. Ltd.	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	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. Options to give consent	Notice should be given in standardised format before allowing access to website or application. Notice should list personal data being collected,	__

		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.	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.	the purpose and the list of third party registered data controllers with whom such information may be shared. There should be responsible sharing of personal data should be there. Mandatory enquiry into the cause of the breach should be there.	
22.	KOAN	The definition needs amendment. There must be safeguards in the form of anonymisation of data.	User consent continues to be the legal basis for sharing of personal data. However, processing should be based on alternatives like legitimate interests, performance of contract and processing to protect the interests of the data subject, or where the processing is necessary for compliance with a legal obligation to which the organisation is subject.	Users must be made aware of the monetary value of their data and also the risks associated with sharing certain data on their rights and obligations.	__

23.	Internet Freedom Foundation	Recasting of definition of personal data is cautioned against.	Consent is very important in any data protection regulation. However, user continues to have rights over their data even after its collection to have to ensure the principle of consent is meaningfully given to users, accountability systems need to be implemented by adoption of a, “privacy by design principle”.	__	__
24.	Mozilla Corporation	Two international examples must be taken into consideration for defining personal data. First, the EU’s General Data Protection Regulation (GDPR) definition of personal data, which is particularly valuable for its detailed articulation of indirect identification. Second, the International Principles on the Application of Human Rights to Communications Surveillance - also known as the Necessary and Proportionate	In regards to the question of consent, users should generally have to give explicit, informed, affirmative consent for their personal data to be used/processed/etc. 1. The stakeholder has directed the attention towards the following six grounds for processing of data.1. The data subject has consented 2. Processing is necessary for performance of contract 3. Compliance with a legal obligation	Privacy notices must written in clear, accessible language. Privacy notice should also be provided in each language that the service is offered. It must be specified when consent must be obtained and what types of data processing actions require consent once versus at every instance of access, storage, or processing.	__

		Principles - contain a definition of "protected information."	4. To protect vital interests of the data subject or other persons 5. For a task carried out in the public interest. 6. The legitimate interest of the controller. The stakeholder however, recommends that legitimate interest either not be included in any forthcoming regulation or that strict safeguards are enacted in order to ensure that legitimate interest does not become a loophole that renders data protection meaningless.		
25.	Internet Democracy Project	The definition should be expanded to include communications content and geolocation information also. The definition of 'sensitive personal data' should be accommodative of the fact that depending on the context, innocuous fields of data can become sensitive.	'Sensitive personal data' that is not essential for a service should not be collected without explicit opt-in consent.	Supplement the privacy principles noted in the consultation paper with data portability and accessible redressal mechanisms.	Create incentives for pseudonymising data, so that the benefits that might accrue from processing user data for specific purposes may be balanced with allowing users the choice of not

					sharing identifiable information.
26.	Citibank	Personal data should be expanded to include the other categories like call details records, calling patterns, location data, data usage information, details relating to browsing, usage of Apps, etc.	It is prudent to mandate the User's consent before sharing his/her personal data for commercial purposes. The users can be empowered to own and take control of his/her personal data by implementing under the Indian telecom regulatory framework the principles like Choice and Consent (opt-in/opt-out), Access and correction etc. as recommended under the National Level Privacy Principles.	The data controllers need to be imposed with the mandate of giving simple to understand Notice of its information practices to their users in all their services, alongwith grievance redressal mechanism on any claims of users on the same. Further, the consumers/users could be granted with the right to demand information of their respective data controllers/service providers from the records of the regular like TRAI etc.	__

27.	iSPIRT	Personal Data should be defined as any data linked to a specific user through any of the identifiers associated with that user.	Informed user consent for collection of data should be a mandatory requirement for collecting data from users and there must be a mechanism for users to opt-in or opt-out of the data collection.	Following measures must be taken. Make the user's telecom data (as defined by TRAI) available to users (in a digitally signed and machine readable format with ability for the users to view/print in human friendly format) via email or a telecom company's website. In case of multiple users linked to data, each user is permitted to share that data further with only their individual consent. Some fields may be protected to eliminate privacy of the other party. In accordance with the Digital Locker System, put the user's data	—

				into their Digital Locker on a periodic basis. In accordance with the Electronic Consent Framework, put the user in control of their data by making it accessible for safe and secure consented data sharing with other service providers as determined by the user. An immutable and auditable record must be implemented for data being accessed in the interest of national security, based on a lawful process, and such access must be reported publicly at a monthly interval by each service provider.	

				User education will also be required to make the users aware about the risks and benefits of sharing their data.	
28.	The Centre for Internet and Society (CIS)	The definition of personal data should be clarified to include data actively provided by the data subject, observed data (data that is provided automatically by virtue of the use of the service) and inferred data (data created by the data controller on the basis of provided data, ie, profiles based on inferences).	Consent should be taken before sharing a data subject's personal data for commercial purposes, and the names of the third parties should be disclosed. Companies should be prohibited from refusing services to consumers who do not consent, and consent should not be a condition precedent for the provision of the service unless it is essential to the service being provided.	Users should have the following rights: 1. Right to an easy-to-understand privacy notice. 2. Right to withdraw consent. 3. Right against unfair denial of service. 4. Right to access, which would include the right to know the specifics of the processing of data and the entities involved, as well as access to data observed about the data subject. 5. Right to data portability.	—

				6. Right to access when data is indirectly obtained. 7. Right to access data about previous breaches. 8. Right to deletion.	
29.	US India Business Council (USIBC)	The Indian definition of personal data is in line with international norms. We recommend that India ensure that "Sensitive Data" and its specific applications be well defined to avoid any ambiguity and uncertainty. Further, there should be reasonable exceptions to the prohibition of collecting sensitive data, such as when the data is made public by the data subject, when data is being used for historical or research purposes, or when the data is necessary to exercise a right or obligation under the law. Personal data should not include anonymised data.	There should be a "notice principle" that ensures data subjects receive notification about the type of data to be collected and how they will be put to use. As India is a multi-linguistic country, any consent and terms of consent provided only in English or Hindi will be limiting data providers' ability to comprehend the details. Data collectors should voluntarily provide the consent form and terms of consent in the language of the user and or the language of choice. Data should be subject to access rights and data security obligations, users of that data	__	__

			should not be subject to all consent requirements. Since the data is obtained from public sources, obtaining consent is not feasible since the user does not interact with the data subject. Finally, while consent is an important ground for processing data, consent should not be the only ground for processing data. In particular, express consent should be limited to situations where consent is the sole basis for collecting and processing data. Provisions related to consent in general should consider the context of the data processing and allow for a flexible approach to avoid confusing consumers with repeated requests for consent in often trivial situations. Any framework needs a range of options which can be applied pragmatically and in appropriate contexts to enable the full range of beneficial data uses in the		

			modern information age while also protecting the individual.		
30.	Disney Broadcasting (India) Ltd	Any expansion of the categories of sensitive personal information under Indian law be calibrated to the risk of harm to the individual, as well as the reasonable expectations of individuals regarding the collection and use of their data.	Requiring specific user consent is not appropriate in all circumstances - some types of data collection and use are consistent with user expectations, and the context of the transaction should be allowed to proceed without asking for additional user consent. For example, an entity should be able to use third party vendors to collect or process data on the entity's behalf if the use of the data is well controlled and otherwise consistent with the consumer's expectations.	There must be easy to use consent mechanisms in place. Centralised consent relieves consumers of the need to configure multiple, individual controls. Likewise, customers of a platform provider may also benefit from a centralised control mechanism that would allow them to give consent at the platform level for data collection and use that takes place with individual applications on that platform.	__
31.	Business Software Alliance (BSA)	The definition of 'Personal Data' should be limited to data that is reasonably linked to an	The standard for obtaining consent should be contextual. Apart from Consent there must be other legal basis for 'handling'	__	__

		identified or identifiable natural person.	personal data including for the legitimate interest of companies handling the data where obtaining consent may not be suitable or practicable, the performance on contracts with the data subject, and compliance with legal obligations, among other things.		
32.	IT for Change	Defined as as any such data which, whether by itself or in combination with other data, can identify a person, is appropriate for the purpose of privacy protection. But, even for this purpose, its implications requires greater elaboration as for instance provided by Opinion 4/ 2007 of EU's Data Protection Working Party.	User's consent should be taken before sharing his/her data for commercial purposes. However, consent does not provide adequate protection so there is a need to go beyond the consent based approach to privacy and user's control over her/ his data.	These consist in defining the ownership patterns over various kinds of user generated data, and defining what constitutes such data (and other categories like data that is further developed from/ over user generated data). Need to define the ownership rights to data in cyberspace just as rights are defined in physical space.	__

33.	SFLC.in	Meta data should also get the same kind of protection as that accorded to personal data. Meta data about communications, can be used to gather information about a person.	User consent is necessary before sharing her personal data for commercial purposes. Sharing of data without any checks would result in violation of an individual's right to privacy. Certain measures should be taken to empower users to take control of her data. These include (a)System in place should be an opt-in system instead of an opt-out system. Rules should be instituted that require individuals to opt in before companies or government entities can collect, use, and share their personal information. (b) There must be simplification of privacy notices so that the user may understand what data is taken, who it is shared with and who can be approached in case of a grievance. (c) Consent of the user must be taken before transferring the data to third party.He should be given an option to opt out of the	(a) Ability to initiate proceedings against a data controller or data processor) even if no wrongful loss or wrongful gain can be shown. There is a violation of privacy even when there is collection, use, disclosure or retention of personal data without consent. (b) Consent cannot be taken as a defence in case harm is caused to the consumers as a result of negligence on the part of data processors or data controller. (c) In case the consumers want to revoke consent at any stage of data collection or processing, they must	__

			transfer within a reasonable amount of time before the data is shared. When data is shared for law enforcement purposes, the user must be informed. Unless user is not informed about the law enforcement access he cannot mount a proper legal defence. (d) 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 provides that any body corporate must not collect sensitive personal data or information unless the sensitive data or information is considered necessary for the purpose. This should be expanded to include all personal data or information	be allowed to do the same. They must be allowed to revoke their consent in respect to all as well as selective data collection and processing activities. Once consent is revoked data controller or data processor must delete the existing data about that consumer. 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 access to	

			instead of sensitive personal data or information. (e)Right to revoke their consent must be given to the users at any point of processing of data. In case of revocation of consent 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. (f) Users should be able to access the data and make corrections to the same. (g)Users should be able to transfer the data from one data controller to another.	data held by a data controller or processor. They must be allowed to correct the data in case the same is incorrect. (e) Consumers must be allowed to transfer their data from one service provider to another at their own choice. In order to make this transfer in a standardised manner, TRAI could mandate a specific format in which the data must be made available by service providers upon consumer request The data must be in both human readable as well as machine readable formats. (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) All the procedure relating to data like transfer of data, revoking of consent etc must be simple.	
34.	EBG Federation	The definition in India is adequate and protects user rights.	Privacy policies to be provided to users explaining how their data will be used and the names of the persons responsible.	__	__
35.	AT&T Global Network Services India Pvt. Ltd.	Personal data falls on a spectrum of identifiability, which should be the primary factor to determine whether information is personal data or not. De-identified or anonymised data should not constitute personal information.	A flexible regime based on the sensitivity of data and how it is used is preferable to one which is based exclusively on consent. Therefore, while people should be given transparency and means to exercise choice and control over collection of data, there should be flexibility which allows for other beneficial uses of data.	__	__

36.	Broadband India Forum	Indian definition in lines with international norms. However, any proposed legislation should recognise the role that purpose, context and proportionality (including voluntary disclosure) play in determining whether a particular piece of information in isolation or in combination with other information constitutes personal information. The definition should provide legal certainty at the same time it must be applied in various contexts proportionally. Proportionality means that the appropriate level of protection is applied to different kinds of information	There should be a regime that puts user in control of personal data and provides flexibility for businesses to use data in certain legitimate ways that further public and business interests. Therefore, the policy should be such that it allows use of data for beneficial uses. Instead of making consent the only basis for processing data, a better approach would be to contextualise the way consent is expressed by individuals according to the kind of service they are using, the sensitivity of the data and to the potential harm arising from its use.	Given that subjective nature of privacy users should be in control of providing necessary information and options to exercise their choice meaningfully wherever relevant. User transparency should be there and consumers should have a single view of what PI is collected and processed by the companies.	__
37.	Sangeet Sindan	Definition of personal data provided under GDPR should be adopted.	The consent of data subject must be taken before sharing his/her data for commercial purpose. This would provide an opportunity to data subject to either object to or provide	For the purpose of capacity building following points should be considered (i) the right of access,	__

			consent for sharing data outside the country.	(ii) the right to rectification, (iii) the right to delete, (iv) the right to restrict processing, (v) the right to data portability, (vi) the right to object (vii) right not to be traced unlawfully based on the personal data, and (viii) the right not to be subject to a decision based solely on automated processing.	
38.	Redmorph	Principles put forward by CIS should be adopted. Advocates for adopting principles put forth by CIS for data collection.	For access to data to third parties and for giving access to third parties to collect data directly, there must be rules laid down. If permission has been given to the app owner that does not mean that permission has been given to transfer the data to third party. For the purpose of data to third	—	—

			parties permission must be taken directly from user.		
39.	Baijayant Jay Panda		1. Express, affirmative and informed consent must be taken from the user before sharing his/her data for commercial purposes. 2. The essential clauses of the contract must be in simplified form so that the customers are able to understand the terms and conditions under which data is used for commercial purposes. The customers must be empowered with the knowledge to know where their data is being used and in case of breach the customer must be informed within a stipulated period of time. 3. The customer should have the right to refuse giving his/her consent. Also, he should have the right to correct the data which is outdated or unwanted.	__	__-

40.	Apurv Jain	__	__	__	__
41.	Reliance Jio Infocomm Limited (RJIL)	Sensitive personal data or information consists of information relating to i. Password; Ii. Financial information such as Bank account or credit card or debit card or other payment instrument details; Iii. Physical, physiological and mental health condition; iv. Sexual orientation; v. Medical records and history; vi. Biometric information; Any further changes to the definition should be technology/ service neutral and should be applicable to all the players in the digital ecosystem irrespective of the organizations origin (based in India or not) or them being under the Government's licensing regime	Explicit consent is necessary for using the data for commercial purposes. The consent taken must be purpose limited as per A.P. Shah Committee recommendations. The Aadhar based eKYC done by telecom service providers could be followed as a case based practice.	The users registered with TSP have sufficient control over their personal data. The provider of personal data is given rights by the TSP to edit the data provided. Unified License conditions prevents misuse of personal data collected.	__

		(or not). Anonymized data being identity less should not be considered as "personal data". There should be guidelines for processing of anonymized data. Such anonymized data will help not only help the policy initiatives but will also result in businesses providing for better user services.			
42.	Bharti Airtel Limited	No change is required in the definition. There should be a difference 'personal information or personally Identifiable Information (PII)' and `anonymized or aggregate data'. While in case of former usage should be allowed only on explicit consent of the user. The later should be allowed to be shared on overarching consent for the usage of services.	Consent should be clear and unambiguous. The privacy rules of any legal entity whose services are being offered or used in the country should comply with the privacy rules of that country. Consumers should have control on usage of their personal information whether commercially or otherwise. Consumers should be able to keep track of all their previous consent given for specific end use. They should also be able to able to manage "opt-in" or	The customer should have the right to seek deletion of all information which has been stored by entity/individual except for the information that is necessary for providing the services by that entity and the information that is mandatory to be stored due to legal/regulatory reasons. Customer	__

			"opt-out" option given for sharing of their personal data.	should have the choice to stop the services and delete the data completely. The entities must not use and store the personal information of the customer, once they stop the service of the entity.	
43.	Idea Cellular Ltd.	The definitions already codified are of great value. However, there needs to be change in definitions of sources, as related to personal data in view of the recent advances in technology. Due to changes in technology sata can be generated by data controllers and processors as well instead of it being collected from user himself/herself. For instance, many mobile applications collect a wide variety of data such as handset information, times of usage, types of usage, location	Proper notice should be given for the purpose of collecting personal information by the entities. Personal data may be used by the entities for providing services as stated in the agreement and also to improve the services or offerings made to the customers. Any other usage beyond this would require explicit consent. The consent should state a. The type of data / personal information that will be collected b. The purpose for which it will be used	An option to opt out of the consent for sharing of personal data should be there. Detailed procedure for the same must be made available to the user. Users should be able to view and edit already granted consent. Each consent should refer to a specific data set, a specific use of the collected personal data and should	—

		information. Each of these pieces of information may not be personal information but in combination they can be used to build individual's profile. There should be no difference between user provided or system generated information.The principles of data privacy should apply to all data that qualifies to be "personal Information" by nature. In case of data that is anonymized or aggregated in nature, there should be no requirement of user consent. For the purposes such information declarations should be made as a part of the Organizations' Privacy Policy where the intended use of such information and the categories of recipients can be mentioned.	c. The consequence of data being used d. The retention period for this data e. The Data Processors, if any, that will be involved in the data being used, which will have access to this data. The liability of collection and storage of user consent and also consent for sharing of data with any Data Processor should lie on the Data Controller, or the entity directly interacting with users.	clearly state how that data will be used. Also, whether any Data Processors will be provided that data for the noted use and how long the data will be retained. Inter application data transfer should be enabled which must be compliant with data protection laws. Data protection framework should specify when consent must be obtained, and what types of data processing actions require consent once versus at every instance of access, storage, or processing. Data processing actions should be permitted with (1) the consent of the	

				data subject or (2) when it is necessary for the provision a service.	
44.	Mahanagar Telephone Nigam Limited (MTNL)	Definition of personal data should include the information that involves the data of any third person such as phonebook contacts.	Consent is mandatory before sharing of personal data of a user. Customer must be explained in detail about the purpose and impact of sharing of data. The following measures are suggested Whenever any user's personal data is proposed to be used, a message should be sent to such user for their denial or acceptance. Despite a user having had given his consent to use his / her personal data, a user should have mechanisms to ascertain who are the users of his / her personal data and should have the right to modify the use of data. No third party should be allowed to utilise a user's data without	__	__

			specific permission from such user.		
45	Reliance Communications Ltd.	Following items must be added to the list of information related to personal information a. Online Activity. b.Information stored in personal devices. c.Information obtained from personal use M2M devices like health devices, connected cars, e-meters, etc.	User's explicit consent should be taken before sharing his / her personal data for commercial purposes. There is an urgent need for strict enforcement of Rules 5 and 6 of the IT Rules 2011 for ensuring that due permission is taken from each user before accessing and sharing of his / her information for any use.	Though licensing would be desired for exercising better control over the use of users' personal data, however, for the sake of providing an environment conducive for innovation, it is recommended that if any mobile app indulges in collection of personal data of the users they should be mandated to register themselves with TRAI. For ease and simplicity sake, this process for registration should be made online. While registering the app should be obligated to elucidate the reasons	__

				for which the app intends to collect the users' personal data.	
46.	Tata Teleservices Ltd. (TTL)	Personal data should cover all aspects of personal data and does not require any changes. Sensitive personal data must be expanded to include racial or origin, political opinions, philosophical or religious beliefs, offences committed or alleged to have committed, prosecution taken, convictions obtained and punishment imposed.	Explicit consent be taken for processing or sharing of information for commercial as well as non commercial purposes. The only exception is under specific legal obligations. Right should be given to withdraw the consent for collecting, processing and sharing personal data, unconditionally, unless it falls under lawful obligations of the data controller.	__	__

47.	Bharat Sanchar Nigam Limited (BSNL)	Personal data should include the personal details which identify the personal characteristics of the data subject Family, lifestyle and social circumstances Education and training details Employment details Financial details Goods or services provided	Consent must be taken before personal data is processed for commercial purposes or for other purposes than for which the data was collected. Personal data should be collected for limited and lawful purposes. It should be shared with only law enforcement agencies for security purposes. Personal data should not be transferred to a territory outside India that does not have equivalent level of data protection.	There should be a right to withdraw the data on leaving the app. Subscriber data must be used for providing better services only and commercial use must be prohibited. Only anonymized and aggregated data should be allowed to be used by the companies that use the data to develop better products.	—
48.	Telenor	The definition of personal data already aligns with international standards. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organizations	The obligation of taking consent of the user would depend on the category of information collected and the sensitivity of information collected. In case personal sensitive information is to be used for commercial purposes user consent should be taken to respect his/her privacy. However,	The best way to empower users is to spread consumer awareness of privacy principles through requirements of transparency by companies, such as through outlining a	Practises already outlined in European guidance on privacy should be implemented in regulatory measures undertaken by countries outside of

		collect information about people.	in case of anonymized data and / or data available in the public domain being processed, there is no requirement of user consent.	clear and accurate privacy policy and opt-outs for data usage. It will help users to take control of their personal data and withdraw the consent given earlier. made for availing specific service(s).	the EEA. This is to ensure consistent global regulations needed for the increasing uses of crossborder data.
49.	Vodafone	The definition given in IT Act is sufficient and should be continued with.	Regulation or protection of that data should be there that results in identification of the individual. Anonymized usage of data must not come under the purview of any regulation. Consent should be taken before the data is shared in user identifiable format with any third party for commercial purposes.	Data protection, security and privacy policy of every company, entity and digital player must be in the public domain. The policy may describe the type of information collected, the purpose of use of the information, to whom or how the information can be disclosed and the reasonable security practices and	__

				procedures followed to safeguard the information.	
50.	Federation Of Consumer And Service Organization	__	Written consent of a user mandatory before sharing of personal data for any purpose.	__	__
51.	Consumer Unity & Trust Society(CUTS)	The definition of 'personal data' should include consumers' passive data. This raises the important question of adequately defining/classifying various kinds of consumer data, such as qualitative data, descriptive data, preferential data, quantitative data, identity data, anonymous data etc. All of the above must be protected through different methods.	Consent of the user should be taken before sharing their personal information for commercial as well as non commercial purposes.	Measures taken to establish control /ownership over one's data must be both regulatory and technological. Consumers must be made to understood about how their data is being used by data controllers and for what reasons. A consumer awareness generation programme should also be launched along with an intent to have a strong redressal mechanism.	__

52.	Consumer Guidance Society	Personal data should be widened to include data secured by broadband service providers, mobile set manufacturers, device and software appliance developers.	Consent of the user must be taken before using his/her data for commercial and trade purposes. Personal and sensitive information should only after taking user into confidence.	1.Except for investigation, national security and other reasons for state and national security there should be complete confidentiality of data. 2. User being the title owner of his/her data should have the right to amend the same. 3. Personal or sensitive information should be disclosed only after taking user into confidence 4. Rules and regulations must be in place for information privacy and the same must be recognised as fundamental right.	__
53.	Consumer Protection Association	Personal data can be defined as any information relating to an identified or identifiable natural person. An identifiable natural	1. Clear, affirmative consent (given by a clear affirmative act like a written statement including by electronic means or an oral	Right should be given to take collective actions pertaining to the enforcement of	Following should be the rights of the consumer vis a vis data controllers

		person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person	statement) should be there when the data is collected. 2. Right should be given to withdraw the consent at any time.The consent withdrawal shall not affect the lawfulness of processing of data before the withdrawal of consent. 3. Consent withdrawal should be as easy as giving consent. 4. While assessing whether consent is freely given account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. 5. When the data is processed of a child who is below the age of 16 years the same would be	the act. The individual should have right to judicial remedy if supervisory authority does not respond within one month on the progress of the complaint. The individuals should have the right to judicial remedy if they consider that their rights have been infringed upon. Also, there should be a right to compensation for damage suffered. The individual should have the right to request from the supervisory authority that the processing is lawful. Penalties should be imposed by the authority.	1. Data controllers should inform when data is collected. 2. Consumer should know the name of the controller, what the processing is going to be used for, to whom their data may be transferred 3. Consumers should be informed whether the data was obtained directly or indirectly unless this information proves impossible or too difficult to obtain, or is legally protected. 4. Right to ask if data controller is processing personal data about you.

			lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.		5. Right to receive a copy of this data in intelligible form; free of cost.