TABULAR MAPPING OF STAKEHOLDERS' RESPONSES TO THE TRAI PRIVACY CONSULTATION PAPER: PART VIII OF XII –KEY ISSUES PERTAINING TO PERSONAL DATA COLLECTION AND USE

The following table was prepared after an analysis of all fifty-three (53) responses to question 9 of the Consultation Paper: "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?" 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 the White Paper namely, the approach for framing a data protection statute, consent as the basis for processing of data and the principles informing and limiting the mechanisms for data collection.

S. No.	Stakeholder	Issues			Recommendations	
		Separate data protection statute equally applicable to all types of service providers	**Consent based opt-in/opt-out mechanisms as legitimate basis of data collection.**	**Other Issues Highlighted**	**Principles for data collection and use**	**Other recommendations**
1.	**Internet and Mobile Association of India (IAMAI)**	Neutral data protection law that could be applicable across various industries and service provider is suggested.	Users to be made aware of the consequences of parting with their data. Law to focus on creating user awareness.	a) Distinction between responsibilities of data controller and data processor b) Threat to innovation by regulations	Following the APEC Principles is recommended.	a) Permitting large scale data collection and storage in accordance with the mentioned principles; b) Modification of, the 'notice and consent model' to allow simultaneous data sharing for the IoT to flourish.

				on data portability.		
2.	**Association of Competitive Telecom Operators (ACTO)**	-	-	Lack of distinction between sensitive and personal data in data protection statutes.	Best Practices based on APEC and OECD frameworks.	Data protection law should distinguish between sensitive and personal data, and accord special treatment to some forms of personal data.
3.	**Associated Chambers of Commerce and Industry of India (ASSOCHAM)**	A technology and platform neutral data protection law is the way forward.	It must be ensured that user choice and volition are respected to the maximum extent. Users should have the option to opt out of certain services.	-	-	Need to maintain balance between innovation and respect for user privacy in the usage of data.
4.	**Cellular Operators Association of India (COAI)**	Harmonise data protection requirements under single data protection law, which is applicable to all players in the ecosystems.	-	-	-	-
5.	**Global System for Mobile Communications (GSMA)**	Horizontal, principles-based rules are needed for all stakeholders operating in the Internet ecosystem; Governments should ensure legislation is service and	-	Need to impose duty on all service providers for maintaining confidentiality of user data.	Necessary safeguards should be derived from a combination of internationally agreed approaches, national legislation and industry	a) Data protection law should not favour innovation against privacy b) Regulators to clarify with consumers about what they do protect, and what consumers should expect in terms of privacy c) Make clear what

		technology-neutral, so that its rules are applied consistently to all entities that collect, process and store personal data			action	they have no control over, such as third party applications and services.
6.	**Internet Service Providers Association of India (ISPAI)**	The rules pertaining to privacy and data protection of personal data should be equally applicable to all the entities operating in Internet ecosystem irrespective of the technology they use and nature of services they provide.	-	-	-	-
7.	**National Law University, Delhi.**	A horizontal data protection law, and is applicable to all stakeholders should be put in place.	-	Concerns over jurisdiction of TRAI to legislate on data protection. TRAI's powers are limited to making recommendations and regulating telecommunication services and service providers. In this context, any regulation on data protection	European Standards' i.e. those set out in the GDPR may be adopted as the base for any new regulations so as ensure that India has greater chances of being recognised as having 'adequate' data protection frameworks by the EU,	-

				implemented by the TRAI may not be applicable to many of the other stakeholders referred to in this question	and improve trade relations with the EU and other countries that adopt similar standards.	
8.	**Span Technologies**	Need data protection law to provide standardized processes to be followed by all entities sharing data.	-	Setting up a data protection authority to look into violations of privacy and provide redressal	-	Service providers should mandatorily have local servers.
9.	**TRA**	-	-	-	-	-
10.	**The National Association of Software and Services Companies (NASSCOM) - Data Security Council of India (DSCI)**	Having a technology/platform neutral data protection law which applies horizontally across the ecosystem should be the way forward	Recommend providing explicit and unambiguous consent from the users for PII and sensitive data sets	a) Failure to have the appropriate legal authority to collect, use or disclose personal information; b) excessive collection of PII (loss of operational control); c) unauthorized access to PII (loss of confidentiality); d) unauthorized modification of the PII (loss of	-	a) Users should be provided detail scope where his data would be used for. b) Self-certification on privacy policy and practices c) Notifications to the users in case of any changes; d) Provision of a single dashboard on devices, platforms, systems, apps etc. to provide end to end visibility on privacy settings and on its control

				integrity); e) loss, theft or unauthorized removal of the PII (loss of availability); f) unauthorized or inappropriate linking of PII; g) failure to keep information appropriately secure; h) retention of personal information for longer than necessary i) processing of PII without the knowledge or consent of the PII principal (unless such processing is provided for in the relevant legislation or regulation j) and sharing or		

				repurposing PII with third parties without the explicit informed consent of the data subject		
11.	**The App Association (ACT)**	-	Considering the Indian consumers' ability to give informed consent to various uses of their data in drafting privacy rules.		Adopt rules aligning with the FTC's privacy framework, the ISP Privacy Principles, and advise against emulating aspects of the GDPR widely regarded as unduly imposing compliance obligations without a corresponding benefit to the public and/or are technically infeasible	Require strong technical protection mechanisms, such as end-to-end encryption techniques to keep users safe from cyberthreats.
12.	**Zeotap India Pvt. Ltd.**	-	-	-	-	a) Device manufacturers, operating systems, security system and other value add service providers must be asked to implement "privacy by design." b) They must be held responsible for any data breach due to

						their systems, software or otherwise.
13.	**Takshashila Foundation**	Cannot envisage all issues as new stakeholders may crop up. Therefore prudent to create a broad data security framework that addresses the safety of data at rest and data in transit.	-	-	The framework can be based on certain fundamental principles, such as accountability, security, and autonomy	The data protection framework must be cognizant of the Supreme Court's recent ruling on privacy as a fundamental right under the Constitution. Once these foundations are in place, the jurisprudence around data protection can be developed on a case by case basis.
14.	**Information Systems Audit and Control Association (ISACA)**	-	Recognition of the right to be forgotten and the users' right to to cease dissemination of their data held through consent.	Need to consider the responsibilities and requirements of both data controllers and data processes, with the focus of the latter on on security measures and deleting data held in backups, beyond the length of time required to keep the information for the purpose that it was collected.	-	a) Multiple stakeholders should consider mapping the data collection the implications of its aggregation. b) Efforts should be made towards protecting customer privacy and the prevention of unintentional aggregation. c) TSPs and other service providers should carry out privacy impact assessments in a transparent manner.
15.	**International Business Machines Corporation (IBM)**	-	Apps should be required to have consent based data collection,	a) Restricting govt access to user data; b) b) Subjecting data	-	Regulations must evolve appropriate definitions, and take into account measures for consent and data portability.

			and data usage only for purposes consented to; Search engines have to operate according to consent.	owners and collectors to same regulation.		
16.	**Make My Trip**	Existing regulations are not equally applicable to all stakeholders.	-	-	-	Regulations have to create minimum standards to be followed for data collection and processing by stakeholders, subject to third party scrutiny.
17.	**Access Now**	A general purpose, horizontally applicable data privacy law applicable to every entity which, for any purpose and through any means, acquires data is suggested.	-	a) Use of supercookies to secretly monitor the web browsing habits of their users. b) Need for distinguishing between different kinds of online tracking	-	a) Create technologically neutral obligations and safeguards around the use of tracking tools and techniques in general, rather than targeting a specific technology b) Regulation should apply to communications data using electronic communications services and public communications networks such as hotspots to maintain confidentiality of users' communications across such networks. c) Need to recognize the market forces within different categories driving development of features that enhance

						privacy and choices to users.
18.	**US- India Strategic Partnership Forum (USISPF)**	Havinga technology/platform neutral data protection law which applies horizontally across the ecosystem should be the way forward.	-	-	-	-
19.	**Information Technology Industry Council (ITI)**	Data protection requirements applicable to all the players in the ecosystem" must stem from, and be enforced by, an agency or regulatory body are required.	-	-	Various models for regulation can be considered such as: a) Single comprehensive legislation like the EU GDPR. b) Multiple sectoral laws and regulators like the US c) (c) Multilateral accountability based model like APEC.	-
20.	**Sigfox**	High and undifferentiated security or data protection requirements for all applications can create negative effects for innovation.	-	The need for the adaptation of the protection mechanisms to a) the kind of data protected,	-	a) The government should promote privacy-by-design and security-by-design principles throughout the development, implementation and deployment cycle.

				i.e. Personal Data or non-personal data together with; b) the context of the processing, like the provision of a subscribed electronic communication service; c) the effective control of the stakeholder on such data.		b) Piracy-by-design principles should also be applied to the development of standards, applications, services, and business processes.
21.	**Exotel Techcom Pvt. Ltd.**	-	-	-	-	-
22.	**KOAN**	-	Development of consent based norms to reflect the growing use of machine-to machine applications and big data applications to exchange information /	-	-	Development of emerging technologies should not unnecessarily be hindered by onerous requirements.
23.	**Internet**	A	-	Lack of	-	Need for reform on the

	Freedom Foundation (IFF)	comprehensive data protection law enforced by an independent data protection authority with investigatory and enforcement powers is the best mechanism to protect data pertaining to the collection and use of data.		TRAI's s jurisdictional ability to determine norms for content and application service providers		prohibition of use of bulk encryption as is presently contained in Clause 37.1 of the UAS license.
24.	**Mozillla**	Data protection obligations and responsibilities should apply to all actors.	-	-	In addition to the principles outlined in the AP Shah Committee Report the following must be incorporated in a data protection statute: a) Data breach notification; b) Enforcement and oversight c) Right to object; d) Data portability e) Privacy by design.	-
25.	**Internet Democracy Project (IDP)**	-	-	Lack of competence and jurisdiction of TRAI to regulate a data protection framework framework	-	-

				applicable to content and OTT service providers.		
26.	**Citibank**	-	Focus on how the data, which are already collected and being used by the other stakeholders, can be protected in light of the impugned consents that are obtained from their users hitherto.	-	-	a) Creation of data sandbox under the technology enabled architecture of personal data. b) This mechanism has to be coupled with punitive consequences in case of non-compliance.
27.	**Indian Software Product Industry Round Table (iSpirit)**	Data protections have to apply uniformly to all entities that handle or process user data.	-	Lack of TRAI's jurisdiction to impose data protection requirements on all stakeholders concerned.	-	-
28.	**The Centre for Internet and Society (CIS)**	Technology and platform neutral data protection law to apply to all service providers.	-	Harmonisation of Unified License with data protection law.	-	Encryption requirements have to be minimal so that data protection may be privacy protecting and enhancing, not privacy limiting.
29.	**US India Business Council (USIBC)**	-	Creating a balance between empowering the individual to exercise choices	-	Refer to EU GDPR for legal bases for data processing that do not rely on consent.	a) Legitimate interest should be the legal basis for collection of rather than consent; b) Implied or informed consumer consent for data use and

			about their privacy and not overloading privacy policies with too much detail that can confuse consumers or cause them to ignore the policies altogether. Need to recognise that consent may not be feasible at all times. Further, consent to be implied for commonly accepted data collection and use practices			transfer, rather than express or affirmative consent, is an appropriate default. c) For cases of cyber crimes and where consent hard to find, legitimate interest basis to apply.
30.	**Disney Broadcasting (India) Ltd**	-	-	-	-	-
31.	**BSA**	-	-	Need to ensure data driven operations not curtailed by restrictions on data transfers in the interests of innovation and growth.	-	Stakeholders should consider flexible, pragmatic approaches to achieve the dual goals of protecting privacy and spurring innovation. Such approaches include recognizing a variety of legal bases for processing personal data, developing a contextual approach to

						the role of individual consent, and implementing an accountability-based model for global data transfers.
32.	**IT for Change**	-	-	-	-	-
33.	**Software Freedom Law Centre (SFLC)**	-	-	a) 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.	Recommendations given by the AP Shah Committee can act as a good guideline.	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. b) All 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. c) Consent should be explicit and clear; d) Browsers must not be allowed to: i) transfer browsing history, cookies, cache data and form data from the local device for any purpose other than syncing

				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		across user devices; ii) interfere with security of data transfer by replacing security certificates; e) Users should have the ability to easily block all web based trackers and advertisements to protect their privacy

				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.		
34.	**European Business Group Federation (EBG)**	-	-	Need to distinguish between data controllers and data processors for determining responsibility in cases of data breach.		
35.	**AT&T Global Network Services India Pvt.**	Need to have consistent privacy regulations applicable to all	-	-	-	Privacy rules should provide level playing field and avoid confusion.

	Ltd. (AT&T)	players to avoid confusion to consumers and enhance customer satisfaction.				
36.	**Broadband Internet Forum (BIF)**	Having a technology/platform neutral data protection law which applies horizontally across the ecosystem should be the way forward.	-	-	-	Need to recognize the market forces within different categories which are driving development of features that enhance privacy and provide more choices to users. For e.g. many browsers today provide incognito mode, do not track features to users; App permissions can easily be controlled by the users.
37.	**Sangeet Sindan**	-	-	-	-	a) The scope of services collecting data should be minimized commensuration to the purpose. b) Express statement by the service providers as to nature and types of data collected by them. c) Details of data protection officer and mechanism of grievance resolution d) The method of accessing the personal data and to ensure the accuracy of the same. e) Express statement about the purpose of collection and usage of personal data to be unambiguously communicated to the data subject within

						reasonable time period and prior to enforce so that the consent from the data subject can be procured. f) Method of withdrawing the consent for processing of the personal data. g) Justifiable and reasonable method of obtaining the consent of the user or data subject before installing the personal data. h) Clear system of identifying whether the communication through the equipment, or mobile application is done in encrypted form. In certain web browsers encryption level can be identified. i) Choice or option in selecting needed and unneeded functionality e.g. in social media application if one wants to disable the location tracking function, however, wishes to keep on other function then such option should be available. j) System or method to check that the personal information stored in the mobile devices are encrypted k) Period of retention

						of personal information and the method of destruction and confirmation post deletion
38.	**Redmorph**	-	-	-	-	-
39.	**Bijayant Jay Panda**	An overarching data protection regime required for data security.	-	-	-	There needs to be responsibility on data handler and processors for data protection.
40.	**Apurv Jain**	-	-	-	-	-
41.	**Reliance Jio Infocomm Limited (RJIL)**	It is in public interest that the guidelines for data protection should address all the players in the digital eco-system	-	Need to provide for data localisation for national security, and judicial remedies to the users.	Priniciples of: a) Data localisation b) Data minimzation as recognised under the EU GDPR and the ICO's office; c) Data accountability	Provide data owners with right to object to ensure that the data owner is made sufficiently aware of the commercial interest that comes along with processing of their personal data and would also ensure that the data collected for a purpose is not misused by the collector for any purpose other than that consented for
42.	**Bharti Airtel Ltd.**	The rules related to data protection should be uniformly applied on all the stakeholders operating in the Internet ecosystem	-	-	-	-
43.	**Idea Cellular Ltd.**	There is a need for an overarching framework/legislation that	-	a) There is very low awareness amongst users	-	-

		reaches out to include all organizations and entities in the digital ecosystem that are involved in collection, processing and usage of personal data		about Cookies used to identify user devices and their harmful uses; b) Identification of users and their activities through device finger printing; c) App permissions often allow sharing of information about third persons who may not be aware of the same; d) Control by devices and IoT to collect huge amounts of data; e) Aggregators have the capability to read and store the A2P SMSs, and they can potentially share this information with		

				other data processors who can further monetize this data.		
44.	**Mahanagar Telephone Nigam Limited (MTNL)**	Responsibilities under a data protection framework must apply to all stakeholders.	-	-	-	a) Sharing of information without user consent must be a punishable offence as criminal breach of trust. b) Independent rating agency/ system should be evolved to provide security and reliability ratings to service providers.
45.	**Reliance Communicati ons Ltd. (RCOM)**	-	-	Need to provide opportunity to both licensed and unlicensed operators to generate income by exploitation of user data.	-	Annonimization of data set is an effective measure that must be taken before encouraging the creation of new data based businesses consistent with the overall framework of data protection.
46.	**Tata Teleservices Ltd. (TTL)**	A legislation that is technology neutral and applies to all entities collecting, storing and using personal data.	-	-	National Privacy Principles enunciated by the A.P Shah Committee should be applicable to all entities processing personal data.	a) Service providers should keep user information confidential b) Only information relevant for a purpose should be extracted; c) Users should be made aware of the the threats and consequences of sharing their information.

47.	**Bharat Sanchar Nigam Ltd. (BSNL)**	All stakeholders that act as data processors should be regulated by a law in the same manner as telcos.	The practice of taking consent by app and service providers needs to be regulated under a proper framework.	-	-	-
48.	**Telenor**	All stakeholders in the digital ecosystem should have the same obligations related to collection and use of consumer data. Thus, it is important that TRAI should recommend consumer data protection framework which will be equally applicable to all the stakeholders ensuring level playing field.	-	-	-	-
49.	**Vodafone**	There is no parity in the data protection requirements and different rules apply to different players. There must be level playing field for all stakeholders.	-	-	-	The proposed rules should not be over restrictive – they must balance the customer's privacy and data protection requirements with the need to facilitate innovative technology based solutions.
50.	**Federation of Consumer**	-	-	-	-	-

	and Service Organizations (FCSO)					
51.	**Consumer Unity and Trust Society (CUTS)**	-	User consent must be taken before sharing their personal data, or any of the above-mentioned data with a third party, for commercial, as well as non-commercial purposes, such as processing, analytics, storage etc. A Data Controller firm might have the rights to commercially use a user's personal data provided that the firm has informed consent of the user.	a) No definition of 'personal data' under Indian law; b) Need to empower consumers by giving them control over their data by allowing data portability, etc.	-	a) A wide definition of 'personal data' is required to include consumers' passive data; b) Empowering consumers through data portability, consumer awareness, and disclosure and accountability requirements on the data controller; c) Data protection framework should be should be optimal and promotes competition, and at the same time, does not pose hurdles for future innovation.
52.	**Consumer Guidance Society (CGS)**	-	-	-	-	a) Every entity and person involved in data collection and processing s should be subject to

						mandatory registration and should be mandated to declare their privacy policy wedded to consumer centric that aims at promoting informed choice of consumers and further recognising consumers as the owners of their personal data. b) In order to address these issues a Data Protection Authority should be established with power to regulate over these entities
53.	**Consumer Protection Association (CPA)**	-	-	Use of tracking headers to collect vast amounts of users' personal data, often without their consent, and sharing of the same with third parties for monetary gains.	-	-