Tabular Mapping Of Stakeholders' Responses To Question 4 - TRAI Consultation Paper: Technology Enabled Audit Mechanism

---

The following table was prepared after an analysis of all fifty-three (53) responses to Question 4 of the Consultation Paper, **"***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?"* The table identifies the issues raised by the stakeholders and their stances in response to the question. It also states the suggestions they have made to the TRAI in view of the question posed.

Sl. No.	Stakeholder	Should a technology enabled architecture be created to audit the use of personal data and associated content?	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?	Comments/Suggestions
1.	IAMAI	Any restrictions on the free flow of data such as an 'audit' mechanism is discouraged because: ● It can hamper innovation and the free flow of information and data; ● It is prone to misuse in wrong hands; ● It can expose user information and breach user trust ● It can be very expensive to develop and regulate. ● The growth of internet enabled services can make it cumbersome to ensure the 'audit' of all services	—	—	Market regulations should be based on evidence. As the cost of proactive enforcement is too large, enforcement for breach of data should be reactive. Greater public awareness about the kind of harms that public can face must be generated to enable them to make better informed choices rather than setting up an architecture to actively monitor and audit data controllers. Build understanding among users through education and awareness. Make organizations accountable through self-regulation. Strengthen grievance redressal mechanisms to empower users. Adopt internationally recognized standards for security of data.

		to which Indian customers submit data.			
2.	ACTO	No.	—	—	Focus should instead be on enforcement of existing rules and targeting uses of data that create a risk of harm to individuals. Industry voluntary efforts, best practice codes and multi-stakeholder initiatives accompanied by accountability mechanisms must be encouraged.
3.	ASSOCHAM	A restrictive or compliance-led framework would severely impede businesses looking to innovate and originate cutting-edge data-centric products and services. An audit-based mechanism would drive up compliance costs and erect barriers to the ease of doing business and innovative practices.	—	—	The most effective mechanism to achieve optimal compliance would be by self-regulatory codes and certifications. The current regulatory framework under the IT Rules recognises the role played by industry-led certification as a method of effective compliance with the requirement to implement security practices and procedures. Such a framework drives compliance by harnessing market forces and incentivizes improvements in privacy. In the presence of effective certification programs, privacy practices would ensure the best possible protection for user data.
4.	COAI	Associated consent must be created as creating a technology enabled architecture to audit the use of personal data would be difficult.	—	—	Counter fears of abuse of data by encouraging good practices and transparency. Adherence to rules may be audited by the companies internally, by third parties such as

					accredited standards bodies like ISO for security or by auditing firms. Such audits for data protection and consent certification should be required for everyone in the ecosystem and the format, structure, etc. can be decided in consultation with the stakeholders.
5.	GSMA	Though, technological controls can be put in place by companies to regulate some processes, human intervention is still needed in many cases. Companies must document their policies and processes and adopt principles that increase accountability. For example, integrated auditing to facilitate accountability in industry-led trust marks, self-certification schemes, and Codes of Conduct. While these initiatives may benefit from government support, they should be industry-driven solutions.	—	—	Educate the public to differentiate between personal data, sensitive personal data and metadata. Counter fears of abuse of data by encouraging good practices and transparency. Adherence to rules(in law or from internal policies) may be audited by the companies internally, by third parties such as accredited standards bodies like ISO for security or by auditing firms. Regulators must supervise companies by relying on reports in most cases and reserve their own audit resources for high profile cases or cases posing significant risk of harm. Institute “accountability agents” who work collaboratively with companies, consumers and governments to certify that the privacy policies and practices of participating companies are compliant with the CBPR system program requirements, including adherence to the APEC Privacy Principles, which are based on globally accepted privacy principles.

6.	ISPAI	Human intervention with support of technology based audit architecture, to check and keep track of the consent logs, will help in compliance monitoring and assessment by the entities.	—	—	Personal data must be kept in encrypted format. Entities must follow best practices and disclose any breach to ensure that appropriate and immediate measures are taken by both customers and authorities. Place access controls to ensure that the encrypted data is not easily available and subject third parties handling personal data on behalf of entities to the same guidelines. Adherence to rules may be audited by the companies internally, by third parties such as accredited standards bodies like ISO for security or by auditing firms or by conducting audits on a case-to-case basis at regular intervals.
7.	NLUD	Regular privacy audits, and privacy impact assessments must be conducted to increase data subjects' trust in data collectors and processors and help data protection authorities monitor their activities.	—	—	Such architecture should be vetted and reviewed thoroughly, with a separate detailed consultation, to ensure that it does not enable infringement of the right to privacy. Strong norms and oversight mechanisms must be put in place wherever industry is involved.
8.	SPAN	—	—	—	Not Responded
9.	TRA	—	—	—	Not Responded
10.	NASSCOM-DSCI	—	—	—	Enforcement and governance framework supported by self-certification or self-declaration by the organizations, regulated by a data protection authority through third party audits would enhance

					India's position in terms of data protection and benefit businesses both directly and indirectly.
11.	ACT	—	—	—	Not Responded
12.	Zeotap	Yes.	—	The technology and expertise necessary to supervise the compliance already exists.	A designated body responsible for data protection and cyber security must be created which must define and enhance Codes of Conduct for personal data security from time to time to keep in sync with technology and threat perception. The standard processes involved in the data security must be defined and regularly revisited in a scientific manner to enable the innovation and new business opportunities. Regular third party audit of such processes and systems must be submitted to the concerned authorities as a condition of license. Such mechanisms of technological compliance monitoring should not create more red-tapism and hindrance for innovation and business.
13.	Takshashila	Yes, the audit architecture must be technologically enabled to evaluate the use of the personal data.	Audits will provide visibility to rectify or prevent harmful consequences.	In the context of processing through machine learning algorithms, harm to the data subject could take place over an extended	As the desired regulatory model will assure certain rights to the data subjects irrespective of their consent, there will be no need to audit consent. Auditors should adopt the following staged approach to review the operations of the data controller:

				period of time and, consequently, there is a risk that it could remain undiscovered unless the actions of the data controller are actively monitored. Harms caused by machine learning algorithms are often the result of inherent algorithmic bias which is very hard to detect. Thus, auditors should be capable of evaluating the output of machine learning algorithms, detecting bias and indicating appropriate remedial measures(eg: introduce appropriate	a. Mandatory publication of queries to databases by data controllers: . b. Black Box Audit, i.e., the actual algorithms of the data controllers are not reviewed, Instead, the audit compares the input algorithm to the resulting output to verify that the algorithm is in fact performing in a privacy preserving manner. c. Provide auditor with access to algorithms if the data controller's algorithms appear to operate in a manner detrimental to the data subjects' rights. Open source algorithms must be used where possible to provide such access. As technology evolves rapidly, it would be counter-productive to define strict limits within which an algorithm must function. Rather, it would be best to define broad principles and develop specific restrictions on a case-by-case basis.

				amount of noise to fuzz out any bias caused over time due to a set pattern by conducting periodic reviews of the data controller's algorithms.	
14.	ISACA	It is advisable to create a technology-enabled architecture to audit the use of personal data and associated consent.	—	The Indian workforce must be enhanced and expanded to best address the added responsibilities, the creation of this new architecture would bring with it.	A two-pronged approach augmenting both the human and technological aspects would be of value to both the government and the citizens. A central register containing information for each data controller should be created. The register's information should include, but not be limited to: the name of the data-controller, their organization, the nature of the information collected and the purpose of such collection.
15.	IBM	It is not feasible to create a capable workforce of auditors, nor for auditing systems to keep up with the rapidly evolving technology.	—	Since most of the audit work can be done with technological solutions, question of skilled workforce in this domain is not a	The industry should be allowed to self-regulate based on government provided data standards. Detect unauthorized access of personal data by reviewing audit logs and maintaining chronological records of system activities to detect and investigate privacy incidents. Name audit logs using a clear naming convention. Audit trails which are used to reconstruct and examine a sequence of activities

				priority, however, availability of workforce for data audit is not a concern for the industry given the dynamic and learning nature of workforce in India, and should not be to the Government as well.	that leads to a specific event, such as a privacy incident. Use access monitoring software which provides real time (or close to real time) dynamic review of access activity to detect unauthorized access to personal information.
16.	MakeMyTrip	Given the size and volume of the businesses which can handle data of users, it may be impractical to form a government owned body which audits the usage of personal data and the associated consents.	An audit mechanism based on auditing of minimum standards compliance by third parties will provide sufficient visibility for the government or its authorised authority to prevent harm to user data.	There is no necessity to create new work-force of auditors to take these responsibilities.	Create minimum standards to be followed by data controllers and processors, who should get a third party independent audit conducted on their systems. The scope of audit should include various aspects like: ● Is the business entity collecting only such data which is absolutely necessary for business? ● Are the terms of service clearly worded to explain the manner in which data will be used, the persons to whom the data will be shared? ● Is the consent of the user obtained before the data is collected?

					• Does the user have the option to retract his consent, or to change its terms to broaden or narrow it; and does the business entity follow such revised consents? • Is the system, website, infrastructure and the security framework of the business entity strong enough to prevent of hacking, cyber-attacks by ransomware or other forms of data leakage or harm?
17.	Access Now	No. A technology enabled architecture will be vulnerable to misuse, especially if designed by the industry to audit its own practices of data handling.	—	—	Any measure for privacy protection must be technology neutral and focused on addressing the impact of intrusive technology rather than regulating or prescribing development of specific applications. Set up an independent body to implement the law through participation of the users and service providers. Create a data privacy commission, to provide users with a single point of contact to file complaints, lodge appeals, access remedy for potential violations of their privacy, etc, so as to not be prejudicial to their rights to pursue remedy through other legal and regulatory forums. The Commission should require each SP to designate a Privacy Office to handle complaints, share best practices, receive training, issue an annual report to the Chief Privacy Commissioner, who should then issue a report aggregating results of the complaints process with recommendations.

18.	USISPF	No, as it may not be practical to create a centralized ex ante tech based compliance system given the scale of transactions and players on the internet.	—	—	Build understanding among users through education and awareness. Make organizations accountable through self-regulation backed by co-regulation, seals and certifications. Strengthen grievance redressal. Industry could help the government understand the risks and benefits of technology solutions, business decisions and the impact of particular prospective regulatory paths and and help them make empirically informed decisions.
19.	ITI	No, a range of instruments exist that can supplement a robust and less resource-intensive data protection model than the techno-consent solution. Reliance on audit-based mechanisms and on a workforce of auditors is not an effective or efficient way to promote best practices, nor to avoid or minimize, harm.	—	—	Rather than ex-post, audit-based mechanisms, focus should be on developing incentives for data handlers to develop responsible and privacy protective practices, through accountability based privacy regimes.
20.	Sigfox	—	A self-audit based mechanism run by the industry will support privacy-enhancing solutions while providing visibility to authorities and	—	Global and harmonized privacy standards must be developed, both technical and regulatory. Adopt initiatives towards a self-audit based mechanism run by the industry

			users and prevent harmful incidents.		
21.	Exotel	Having a technology solution is the only way to monitor the ecosystem for compliance. However, with the complexity & diversity of technologies, human intervention is required, which will both be costly and create competition for smaller number of capable auditors.	Audit alone will not suffice. Financial liability for misuse of personal data should be placed to demotivate such misuse.	—	Guidelines, on what is not accepted, will protect the startup community from overstepping the boundaries. There should be a mix of technology solution and human audit: i. Basic technology based test suite to check the hygiene security & audit requirements. This technology audit will also reduce the workload for human auditors. ii. Build a team of "white hats" or human auditors who only check for exceptions as the hygiene requirements have already been vetted. iii. Compliance monitoring should be based on adherence to benchmarks and be fully automated with a technology based solution. The regulators should get into a public private partnership & promote solutions originating in the ecosystem.

22.	KOAN	An industry driven audit mechanism builds on accountability, and is a preferable alternative over a government set up technology architecture.	—	Since, the specific technological capabilities already exist which can be leveraged by individual enterprises, the industry is capable of setting up a workforce of auditors which can undertake such monitoring.	Currently, specific technology solutions for auditing and managing data access permissions are being offered to enterprises for monitoring their data protection compliance requirements. These include: I. Data discovery and flow mapping technologies which can scan data repositories and resources to identify existing sensitive data II. Classify it appropriately in order to identify compliance issues. III. Data access governance technologies which provide visibility into what and where sensitive data exists, and data access permissions and activities. IV. Consent/data subject rights management solutions which help in managing consent of customers and employees, as well as enforcing their rights over the personal data that they share. A cyber risk insurance framework should be explored whereby frequent incidence of data breaches can be directly correlated to premiums that enterprises may be required to pay based on regular performance assessments.

23.	IFF	The adoption of a technical framework without adequate development of a rights based data protection framework being a form of data centralization would pose risks to users. Also, a universal technical solution may become a form of "digital licensing" which would create an unreasonable barrier for entry and innovation thereby hurting internet users.	—	—	User interest must be safeguarded using a mix of proactive reporting requirements, enforcement and adjudication forums. A "privacy by design" principle, administered by an independent data protection authority or a privacy commissioner, should be put in place.
24.	Mozilla	Given significant differences in business models, products/services, data collection practices, and the complexity of algorithms in use today, a singular technology enabled architecture to audit the use of personal data for all actors in the digital ecosystem seems infeasible to impossible.	Audits are not a substitute for actually empowering users with transparency, choice, and consent or a properly resourced, independent regulator.	While a strong DPA should be established and should have the power to audit the practices of data controllers, the creation of a workforce of auditors seems inadvisable. Consider the example of the US subprime mortgage crisis– it was found that the	Creation of an empowered and independent data protection authority. Have strong documentation requirements and reporting obligations around data processing, access, use, and storage actions. Create capacity for dialogue with and determinations from DPA on pre-market entry or new products/features. Data protection authority should be notified before market entry of any and all products, services, and features that collect, store, process, or use biometric data.

				"failures" of the Big Three rating agencies were "essential cogs in the wheel of financial destruction" and "key enablers of the financial meltdown." Therefore, caution must be practiced before relying heavily on third parties to investigate complex systems and algorithms.	
25.	IDP	A standards driven architecture that can support technology enabled audits can be explored.	—	—	There have however been documented risks associated with automated data processing audits, which should be considered with experts before concretisation.
26.	Citibank	It is superlative to create a technology enabled architecture to audit the use of personal data and associated consent to have methodical check and	Taking into account the huge volume of personal data of individuals involved, an	Sufficiently capable workforce of auditors can be sourced through the statutory professional	—

		balance on the activities of Data Controllers.	audit-based mechanism would be more suitable to provide sufficient visibility for the government or its authorized authority to prevent harm to the users of Telecom sector.	bodies like Institute of Chartered Accountants of India, Institute of Company Secretaries of India, etc. in order to ensure accountability of auditors.	
27.	ISPIRT	Yes, it is advisable to create technology enabled architecture to audit the use of personal data and associated consent.	The audit based mechanism will provide some visibility, but is not entirely sufficient to prevent harm. Hence, it should be created along with a regulatory sandbox for testing out new innovations for rapid evolution of regulations.	Yes, a skilled workforce of data auditors will be required. However, since the data auditors would be dealing with large troves of machine-readable data, it may be possible and desirable to automate large parts of the auditing process using	—

				technological solutions.	
28.	CIS	Audits, compulsory or consensual, are valuable in educating and assisting organization to meet their obligations. Assessment of processing of personal data for adherence to 'good practice', with the agreement of the data controller is known as a consensual audit. Compulsory audits would enable the regulator to serve government departments, designated public authorities and other categories of designated persons with a compulsory assessment notice to evaluate their compliance with data protection principles.	Audits can only look at aspects of procedural compliance and thus need to be complemented with robust mechanisms for redressal and comprehensive policy.	—	—
29.	USIBC	No. A technological audit mechanism is dangerous as it could increase the impact of cyber breaches or unlawful surveillance and is also not practical as it would lead to more regulations.	Creating a framework based around government visibility into an organization's' privacy practices is not consistent with an accountability-based approach which	—	Focus should be on a mechanism that incentivizes privacy protective practices through self-regulation. Organizations should be encouraged to develop voluntary self-enforced risk-based frameworks based on government-established data standards developed through multi-stakeholder consultation Adopt an accountability based approach.

			already includes self-assessment requirements.		
30.	Disney India	—	—	—	Not Responded
31.	BSA	It is not feasible to expect an auditing system to keep pace with rapidly evolving technology. Instead, industry should be encouraged to use available standards and data verification tools.	—	—	TRAI should promote the development and adoption of voluntary, transparently developed, industry-led international standards and recognize certifications from internationally accredited entities.
32.	ITfC	A technology enabled architecture would be beneficial in the current hyper technology-based social architecture, but it would only be useful if there are appropriate laws and regulations in place which are used to enforce them.	—	—	—
33.	SFLC	Technology based architectures do not operate in isolation without active application of mind through human intervention. Harm due to algorithmic biases cannot be prevented in a fool-proof manner, but can be avoided through the use of audits.	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	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	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;

			easily look for errants and help in: ● preventing future security breaches and unintended violations of privacy ● deterring sale of personal data without proper consent	auditors could be developed.	● 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.
34.	EBG	Proactive government monitoring, given the nature, scale and volume of transactions happening on the Internet and multiple players involved in each transaction, may not be practically possible. The regulation itself must allow for positive and beneficial uses of data, this may not be efficiently achieved by creating a technology-enabled architecture to audit the use of personal data and consent.	—	—	Incentivize self-regulation and accountability measures for practices related to privacy protective measures instead of creating a technology-enabled architecture to audit the use of personal data and consent.

35.	AT&T	No, as it may not be practical to create a centralized ex ante tech based compliance system given the scale of transactions and players on the internet.	—	—	Build understanding among users through education and awareness. Make organizations accountable through self-regulation backed by co-regulation, seals and certifications. Strengthen grievance redressal. Also, any policy must recognise that the digital economy is thriving in part because most business work hard to maintain user trust and confidence. Industry could help the government understand the risks and benefits of technology solutions, business decisions and the impact of particular prospective regulatory paths and and help them make empirically informed decisions.
36.	BIF	No, as it may not be practical to create a centralized ex ante tech based compliance system given the scale of transactions and players on the internet. Also, it is not the most effective or efficient way to promote best practices and to ultimately avoid or minimize harm.	—	—	Incentivize privacy protective practices through self-regulation (backed by co-regulation, seals and certifications) and accountability measures paired with explicit legal incentives such as statutory presumptions of compliance and statutory reductions of fines. Build understanding among users through education and awareness. Strengthen grievance redressal. Organizations should be required to develop self-enforced risk-based frameworks which would allow them to focus on high-risk data uses to minimise harms while monitoring low-risk situations.

					Data harms must be empirically proven and mapped before there is further regulation, and any regulation must be narrowly tailored to prevent concrete, identified harms without hindering beneficial uses of data. Also, any policy must recognise that the digital economy is thriving in part because most business work hard to maintain user trust and confidence. Brand safety is a motivation bigger than fear of regulations.
37.	Sangeet	Yes, a technology enabled architecture is very useful and worthy to audit the use of personal data.	—	By capacity building, skill development and training, a capable workforce of auditors can be nurtured. Such capacity building can be achieved through following ways: (i) Certification or diploma programs (ii) Workshops conducted in collaboration with the industrial and	The audit will help the companies to elevate their security levels and prepare the government for new security risks, breach, cyber-attacks and measures to be taken.

				regulatory stakeholders. (iii) Promoting a separate degree or master course in the field of cyber-security or vocational training program.	
38.	Redmorph	Yes, technology enabled architecture can help misuse of personal data. However, it should be used at a data/content usage level and also at an audit level.	—	—	Every app sold in India (free or paid) on Google Play Store, iTunes, etc. should openly declare the network connections made and their country of location, ownership entity, purpose & data collection.
39.	Baijayant Jay Panda	An audit based mechanism will be very necessary, where the powers to audit algorithms and the biases that may come in will lie with the quasi-judicial body.	—	There will be a need for a sufficient workforce with sufficient knowledge of the field.	—
40.	Apurv Jain	—	—	—	—
41.	RJIL	Yes, but architecture designed today might need fundamental changes	TRAI should empanel the following:	The industry would be able to provide skilled manpower to develop, deploy,	The guidelines for data protection should not define the setup but encourage adoption of 'security by design' for implementation of such a setup.

		within a short period of time due to rapid technological advances.	• "Certification agencies" that follow global best practices and can enable the industry players with standardized certificates; • "Auditors" that can help industry with compliance.	supervise, certify and audit these practices which will also result in skill development and employment generation within the country.	Such mechanism should follow the principles of data protection and usage as suggested by the AP Shah Committee. All TSPs should be encouraged to follow global best practices in implementing a state of the art architecture with regular auditing of facilities with the help of internal as well as external auditors.
42.	Airtel	Audit entailing the mix of a technology-enabled architecture and human intervention to track the use of personal data and other information would be an appropriate approach. The technology-based architecture can be used for checking consent logs. Human intervention is required for checking the manner in which the data privacy policy is followed.	—	—	All entities that collect and process the customer data/information should disclose any breach or leakage of any information related to their customers to the appropriate legal/regulatory authorities. All the personal information should be kept anonymous or encrypted and all entities should have access controls to prevent the access of customer or personal information to their employees, affiliates or partners except for specified purposes. All parties, including third parties should be subjected to the same information security guidelines as applicable to the entities.

					The compliance to privacy and data protection law can be assessed by the companies themselves, by third parties(eg: accredited standard bodies like ISO); or by auditing firms. The Government and the Regulators should also supervise the compliance by conducting audits on a case- to-case basis at regular intervals.
43.	Idea	While it could be difficult to create a technology enabled architecture to audit the use of personal data and associated consent, nevertheless such audits by third party agencies could go a long way in creation of a cleaner and safer ecosystem from a privacy perspective.	—	—	Data controllers may be certified as trustable after regular mandatory audits for compliance. However, if only the TSPs are to be held accountable for such audits, only a self-certification should be required of them in view of their proven record. Data should be monitored and access to it logged. All access and utilization should be made available in case of an audit requirement. The requirement may arise due to a suspected or actual breach of data security.
44.	MTNL	Technology enabled architecture to audit the use of personal data should be adopted though 100% abuse of data cannot be prevented with it.	—	The development of the architecture should be done such that the available manpower of skilled auditors can be used for over-riding supervision of	Symmetric regulation for all players of digital ecosystems may help to reduce abuse of personal data.

				exceptional observations collated by the automated systems. Capable workforce can be generated through training and certifications.	
45.	Reliance Communications	Yes.	Yes.	Yes.	—
46.	TTL	There is no requirement to create technology enabled architecture to audit personal data and associated content for TSP's as in order to ensure that customers are protected from phishing attacks, National Customer Preference Register (NCPR) prohibits companies making unsolicited commercial communication with customers, registered in NCPR. Thus TSPs have already put in place adequate security measures to protect their network and data privacy of their customers.	—	—	Putting technology controls in place by entities to regulate some processes would still require human intervention as there will be instances where hardcore computer logics would not work. Hence creating a technology enabled architecture is a vast subject which requires debate involving, over-the-top services, application providers, browsers, operating systems, online payment website, banking websites, e-commerce websites and other stakeholders in the digital ecosystem to study and understand if such an architecture is implementable/executable and auditable, for the government or it's authorized authority.
47.	BSNL	Yes.	—	It should not be difficult to create a sufficiently	An audit can play an important role in the following ways:

				capable workforce of auditors after due training in this field.	a) Educating and assisting organisations/ data controllers to meet their obligations, b) to assess their processing of personal information; and c) to provide practical advice and recommendations to improve the way organizations deal with information rights issues. d) to ensure that the data controller is following good practices. A set of good practices may be defined so that the processing of personal data is carried out in accordance with policies and procedures, systems, records and activities in order to: a) Ensure the appropriate policies and procedure are in place; b) Verify that those policies and procedures are being followed; c) Test the adequacy controls in place; d) Detect breaches or potential breaches of compliance; and e) Recommend any indicated charges in control, policy and procedure.

					f) Identity relevant data protection risks within organizations. The benefits may include ● Helping to raise awareness of data protection; ● Showing an organization's commitment to, and recognition of, the importance of data protection. ● Independent assurance of data protection policies and practices. ● Identification of data protection risks and practical, pragmatic, organizational specific recommendations.
48.	Telenor	Creation of a specified audit tool is inefficient, expensive and problematic as: ● the nature of data and consent collection and the rapid advances in technology would make maintaining such a tool and its workforce extremely costly,if at all possible. ● it would open up new possibilities for data hacking, mining, and abuse. by creating additional exposure of consumer data by allowing new access points into the data.	—	Maintenance of workforce would be quite expensive.	Companies must be required to adequately protect this data by utilizing requirements similar to the European Directive. They should implement internal mechanisms for certification of practices being adopted for data protection and submission of compliance to the designated authority annually, akin to the existing security related compliances being submitted by the licensed TSPs.

49.	Vodafone	An audit based approach may not be required / desirable at this stage for the development of an Electronic consent framework.	—	—	Lay down good practices which could include publishing of the Data Protection, Security and Privacy Policy in the public domain/on the website. All data collection & processing entities should obtain certification of their IT systems viz; International Standard IS/ISO/IEC 27001.
50.	FCSO	An audit based mechanism by the independent agencies or TRAI should be put in place.	—	—	—
51.	CUTS	An auditing mechanism similar to the checking of algorithms for distance and fare calculation, by taxi aggregator mobile apps done by Standardization Testing and Quality Certification(STQC) or any other agency authorized by Ministry of Electronic and Information Technology (MEITY), on a one-time basis, can be put in place.	—	—	—
52.	Consumer Guidance Society	Yes, its the need of the hour.	Yes.	—	Self-regulation of the industry doesn't work due to involvement of conflict of interest and therefore such idea should be discarded.
53.	Consumer Protection Association.	Yes.	Yes.	Yes.	—