Tabular Mapping of Stakeholders' Responses to the TRAI Privacy Consultation Paper
Part XII of XII – Technological Solutions To Monitor Compliance

The following table was prepared after an analysis of all fifty three (53) responses to Question 7 of the Consultation Paper, *"How can the government or its authorized authority setup a technology solution that can assist it in monitoring the ecosystem for compliance? What are the attributes of such a solution that allow the regulations to keep pace with a changing technology ecosystem?"*

The 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.

Sl. No.	Stakeholder	Should the government adopt a technological solution to monitor compliance?	How must such a solution be implemented?	How can such a solution keep pace with the changing technology ecosystem?
1.	IAMAI	No. A technological solution runs the risks of: ● resulting in a geofencing of sorts, and should therefore not be used as a means to impose data localisation. ● becoming redundant or obsolete given the pace at which technology evolves.	A self regulatory model should be adopted and the government should only intervene in the event of failure of market forces. It should be based on voluntary compliance, incentivization and swift enforcement which in turn leads to a general increase in compliance levels due to market forces and adoption of best practices to stay competitive.	__
2.	ACTO	Yes, the government can use technological solutions to address important objective such as national security, public safety, law enforcement and preventing harm to children.	__	The government must respond to technological changes through fair, accountable and uniform procedures that govern when and how private

				companies may be compelled to provide information.
3.	ASSOCHAM	No, The diversity of Business models and practices would make it difficult and overly respective to develop a single technology solution for compliance monitoring. It would also drive up compliance costs and erect barriers at a time when a key focus of the government is to improve the ease of doing business and facilitate innovative practices.	An overly restrictive or compliance based framework would severely impair businesses looking to innovate and originate cutting-edge data centric products and services. A self regulatory model would be the most effective mechanism in achieving optimal compliance as it drives compliance by harnessing market forces.	—
4.	COAI	Maybe. Countering fears of abuse of data by encouraging good practices and transparency is important. However, It would be difficult to create a technology enabled solution.	Instead adherence to rules may be audited internally or by third parties, that have the requisite expertise and capacity, such as accredited standards bodies like ISO.	—
5.	GSMA	No, progressive policies and regulations should be adopted to facilitate the growth of the digital economy as a whole and specifically in those sectors that underpin the digital economy, such as Telecommunications, E-Commerce and digital services. Such approaches would include elimination of restrictions to digital trade such as barriers to cross-border data flows and requirements to localise data.	Countering fears of abuse of data by encouraging good practices and transparency is important. Instead adherence to rules may be audited internally or by third parties, that have the requisite expertise and capacity, such as accredited standards bodies like ISO. A self regulatory model should be adopted and the government should only intervene in the event of failure of market forces. Further, regulators must come out with instruments to monitor or regulate in an ex-post approach than creating an ex-ante compliance framework for want of any evident market failure or where industry	—

			players cannot be said to take care of the same themselves.	
6.	ISPAI	Yes, the government has an important role in helping the industry by building the confidence of customer on the usage of his personal data by the entities.	Access controls may be placed to ensure that the encrypted customer personal data is not being made available easily. Third parties must also be subject to the same guidelines. Human intervention along with a technology based audit architecture (for checking and keeping track of the consent logs) will help in compliance monitoring and assessment by the entities. The compliance can be self-regulated by these entities or by accredited standard bodies like ISO for security; or by auditing firms that have the requisite expertise and capability.	—
7.	NLUD	—	—	—
8.	Span Technologies	Maybe.	The Government should make a standardised process to be followed by all service providers using Aadhaar. The government should also order the tech giants like like Google, Facebook etc. to host servers of some key services that are most widely used in the country within India as: 1. it will be in a position to monitor services to ensure that they are complying Indian laws. 2. it will save cost over international pipes because most net traffic to	—

			such popular sites will be within the country.	
9.	TRA	—	—	—
10.	NASSCOM - DSCI	No, technology developments are highly dynamic making technology solutions for monitoring compliance an overwhelming burden.	There should be a self-regulation system along with adequate grievance redressal mechanism. Solutions with suitable capabilities and effectiveness need to be explored as part of a more concerted approach towards ensuring compliance in the ecosystem. An accountability based privacy regime should be adopted.	—
11.	ACT	—	—	—
12.	Zeotap India Pvt. Ltd.	—	—	—
13.	Takshashila Institution	No, the government shouldn't take up the responsibility of creating a technology solution to aid in monitoring. This role can be performed by market based entities such as auditors.	The government must focus on regulation and primary adjudication of matters arising in the ecosystem. This can be achieved through the setting up of an authority, such as the Data Commissioner.	This authority will be tasked with redressal of grievances as well as the development of technology responsive standards of accountability and transparency.
14.	ISACA	Yes, the advances in artificial intelligence, machine learning, and process automation bode well for technological solutions that will enable compliance monitoring at an ecosystem level.	The government must retain the right of access to audit any organisation to review their data privacy processes to assess if they are appropriate and effective.	To keep pace with a changing technology ecosystem all stakeholders must act in concert to explore the best possible path(s) forward and do so in a manner that is

				thorough, comprehensive and rapidly iterative.
15.	IBM	No, it is not advisable to work on a centralized compliance and monitoring approach. Instead, the development and use of new privacy enhancing technologies and methods must be encouraged as part of the risk-based accountability approach to data protection.	—	—
16.	Make My Trip	No, there should be no government owned body which will audit the usage of personal data and the associated consents.	—	—
17.	Access Now	No, any technological solution designed to monitor an ecosystem runs the risk of becoming a backdoor access into data and could in effect undermine the security of the ecosystem.	Regulations must be technologically neutral and not request the industry or users to use a specific standards. The government should not erode the security of devices or applications by introducing a legal requirement for vulnerabilities or by mandating backdoors into products or services. Companies must not be pressured into keeping private data, allow law enforcement to access to it, or retain encryption keys to decrypt the data.	—
18.	USISPF	No, technology developments are highly dynamic making technology solutions for monitoring compliance an overwhelming burden.	There should be a self-regulation system along with adequate grievance redressal mechanism. Solutions with suitable capabilities and effectiveness need to be explored as part of a more concerted approach towards ensuring compliance in the ecosystem. An accountability based privacy regime should be adopted.	—

19.	ITI	No, a universal, across-the-board, technology-based compliance and monitoring approach to protecting privacy must be avoided.	Rather than investing in ex-post, audit-based mechanisms, the government must instead incentivize the development and use of new privacy enhancing technologies and methods as part of the risk-based accountability approach to data protection such as self-regulation, co-regulation, 3rd party certifications, etc.	—
20.	Sigfox	Maybe. However, a centralised and mandatory monitoring solution should be avoided as much as possible.	The government could foster multi-stakeholder collaboration and provide a platform for discussion on issues such as security and privacy implications of IoT, whereby different actors in the value chain can help each other and assist the government to monitor the ecosystem compliance and hence protect consumers, operators, service providers, and the economy in general. Strong compliance principles enforced by efficient ex-post control policies should be relied upon.	—
21.	Exotel Techcom Pvt. Ltd.	Yes, a technology solution is the only way to monitor the ecosystem for compliance given that there are more than one billion telecom subscribers, each of whom might subscribe to one or more services.	The technology solution must be implemented along with human intervention, constituted in the following manner: - A basic technology based test suite to check the hygiene security & audit requirements, which also provides recommendations in case any product fails the test. - A team of “white hats” or human auditors who check only for exceptions as the hygiene	The regulator must encourage solutions from the ecosystem itself by entering into public private partnerships. In such a setup the regulator will only need to manage the requirements while the ecosystem finds a way to keep pace with evolving technology.

			requirements have already been vetted.	
22.	KOAN	—	Encourages adoption of Privacy by design by companies.	—
23.	IFF	No, because: - a technical framework without adequate development of a rights based data protection framework may not provide any solution for data security or individual privacy. - such a system would by itself be a form of data centralisation and pose risks to users. - It could serve as a universal backdoor to all internet applications and services. - A universal technical solution may become a form of “digital licensing” creating an unreasonable barrier for entry and innovation thereby hurting internet users.	Any technology based solution should be individualised to a product adhering to principles of, “privacy by design” and not operate as a general layer such as a, “consent layer” or the, digilocker technology framework.	—
24.	Mozilla Corporation	Yes, robust documentation around data processing, storage, access, and use is a critical component of any strong data protection framework. However, it is skeptical that there is a single technology solution for monitoring compliance with data protection as data protection relies on a chain of integrated actions and responsibilities.	Given the sensitivity of the information that would be contained in such a system, strict data security requirements, including encryption, role-based access control, multifactor authentication, etc., must be put in place. Also, no technology solution can be a substitute for regular and robust interaction between the data protection authority and data controllers and it should hence be supplemented with regular multi	—

			stakeholder dialogues on data protection, which are critical in ensuring that public interest organizations and technical experts can assist in the implementation and enforcement of the data protection framework.	
25.	IDP	Yes.	Systems that adopt privacy by design and privacy be default easily lend themselves to compliance monitoring. Redesigning and standardising collection and processing operations and encouraging adoption of Privacy Enhancing Technologies (PET) can help in creating a technology-enabled monitoring solution.	'Privacy by design and privacy by default' approaches must be considered for sustainable data protection frameworks that can keep up with technological advances.
26.	Citibank	Yes, a technology enabled architecture on the personal data can bring all the data controllers viz., TSPs and other stakeholders in the telecom sector under one roof.	A technological solution can help: ● bridge monitoring of consumer consents ● regulate anonymized data sets created by the regulated companies ● monitor compliance with international standards.	—
27.	iSPIRT	Yes, a standardized and automated technology solution must be used to exchange audit logs with the regulator.	This solution should mandatorily use formats, and interfaces which are openly available for public review, and preferably use open source. TRAI should make use of Regulatory Technology Accelerators and learn from the global experience, to pioneer the next generation of monitoring tools and techniques.	The solution must be reviewed periodically, for new requirements, and to manage newly discovered harms.

28.	CIS	Yes, the use of privacy enhancing technological solutions is key to the governance of privacy in any jurisdiction.	The use of privacy softwares by companies and by users must be incentivized. The following are some technological solutions to privacy which may be explored: ● Sticky Privacy Policies ● Personal Data Stores ● DND Options ● Standardized Privacy Policies ● Privacy by Default	—
29.	USIBC	No, a mandated technology solution could create new, or increase existing compliance hurdles, and could create a user backlash towards “a big brother approach” that adds onerous compliance issues and negatively impact the growth of the digital economy.	A non-technical solutions for monitoring privacy, emphasizing the specific context and self-enforced risk-based frameworks, must be explored. The regulators and data protection authorities must be partners rather than adversaries.	—
30.	Disney Broadcasting (India) Ltd	No, with rapid changes in technology and ever increasing flow of data, a technological solution might be impractical and stifle innovation. It could also raise concerns about government oversight over such audits, unwanted government surveillance and create a chilling effect on consumers’ adoption of new technologies. There should be no technical controls on cross-border data flows. Such controls would alter the internet’s fundamental architecture. That would slow the growth of the internet in India. India’s privacy framework must preserve the flexibility to move data in and out of India.	Instead, a selective targeted enforcement of existing laws coupled with cooperation with the industry should be pursued. Also, the notice and consent model may not be sufficient in addressing data protection challenges brought about by big data analytics and focussing on industry codes of conduct and best practices, through self-regulation, might be the best way of addressing such challenges. The authority must: 1. promote education and awareness. 2. seek feedback. 3. offer guidance and assistance. 4. act judiciously. 5. act transparently.	—

			6. strive for coordination and cooperation. 7. be business and technology savvy. 8. adopt a public-private partnership (PPP) model. 9. collaborate and work with leading industry stakeholders to use the latest technologies to enhance their efficiency, effectiveness and transparency.	
31.	BSA	No, it is likely to be ineffective.	It should instead incentivize the adoption and use of technologies and methods for protecting personal information as part of a risk-based accountability approach to personal data protection.	—
32.	ITfC	Maybe.	It should be an APIs based systems, building over the IndiaStack architecture. Its DigiLocker and e-consent framework elements are especially relevant in this regard.	—
33.	SFLC	No, technologies could change at a fast pace making any solution designed obsolete in no time.	Standards and guidelines must be introduced to ensure that irrespective of technologies, the goal of protection of privacy rights of citizens is taken care of. There must be principles, standards and guidelines in place that would ensure compliance of service providers with the data protection regulation.	—
34.	EBG	No, introduction of a technology solution for monitoring the ecosystem, may create geofences for cross-border businesses.	Industry is best placed to comply with the privacy principles under a self-regulatory	—

			framework and putting users in control is critical.	
35.	AT&T Global Network Services India Pvt. Ltd.	No, being government owned and operated is unlikely to keep pace with the changes in a dynamic system without placing an enormous burden on the government. It could also raise privacy concerns.	Industry is best placed to comply with the privacy principles under a self-regulatory framework and putting users in control is critical. A culture of corporate accountability must be recognized and endorsed.	—
36.	BIF	No, being government owned and operated is unlikely to keep pace with the changes in a dynamic system without placing an enormous burden on the government. It could also raise privacy concerns.	Industry is best placed to comply with the privacy principles under a self-regulatory framework and putting users in control is critical. A culture of corporate accountability must be recognized and endorsed. If a tech-solution is created, it must not create geo-fences or attempt to localize data. There should be no technical controls on cross-border data flows as that would alter the internet’s fundamental architecture and slow the growth of the internet in India.	—
37.	Sangeet Sindan	Yes, it will help keep pace with technological advancements as well as protect stakeholders participating in the digital ecosystem.	The following points must be considered while setting up a technological solution to monitor compliance: ● Mandatory registration of Application Program Interface (“API”) used for transaction related services. ● A statutory obligation should be casted on the payment gateway industries for adopting the latest Payment Card Industry Data Security Standard.	—

			● Artificial intelligence can be used to monitor the trends and patterns of illegal transactions. ● There exist technological tools to block the APIs used for transaction services that are not duly registered with the government authorities. The following are the key attributes of such a technology solution: ● real time reporting of any breach and violation of compliances ● to provide visibility and effective control ● real time assessment of degree of risk of any threat and loopholes in compliances ● prior signal and warning to the business entities which are not complying with the guideline or directions of the regulatory body or government authorities ● an effective and efficient method of receiving the complaints from the user and resolving the issues in a timely manner.	
38.	Redmorph	—	—	—
39.	Baijayant Jay Panda	—	—	—
40.	Apurv Jain	—	—	—

41.	RJIL	No, given the pace of technological advancement, an architecture or setup designed today might need fundamental changes within a short period of time.	There should be a principle led approach to the industry for the design and implementation of such a setup with a focus on concepts like ‘Privacy by Design’.	—
42.	Bharti Airtel Limited	No.	The compliance to privacy and data protection law can be assessed by the companies themselves or by third parties such as the accredited standard bodies like ISO for security; or by auditing firms that have the requisite expertise and capability. The Government and the Regulators should also supervise the compliance of all entities dealing with personal data and may also conduct audits on a case-to-case basis at regular intervals.	—
43.	Idea Cellular Ltd.	No, a single technology solution may not serve the purpose of assisting in monitoring compliance. The solutions may vary depending on the business case.	While setting up a technology solution the following points must be considered: ● Different ecosystem stakeholders are at play and any compliance regulations should apply to not just the TSP’s but any Data Controller in the entire digital ecosystem. ● Compliance should also be sought from Data Processors.	—
44.	MTNL	Yes.	A common data center may be set up at a place with internet service or where the mobile app can be used, where all personal information is kept. The rules for downloading such an app or using the online service must be clearly defined.	—

45.	Reliance Communications Ltd.	Yes.	TRAI should make an endeavour similar to that made by it when it launched a plethora of apps for speed testing, reporting of UCC, etc.	__
46.	TTL	No, but it extends support for introduction of any measure taken by the government for the objectives of monitoring stated in the question.	__;	__
47.	BSNL	Yes.	The technology solution should: ● Be a privacy enhancing technology. ● Use identity management systems. ● Store consent in an encrypted form from all users. ● Influence privacy norms.	__
48.	Telenor	No.	It should be the responsibility of each partner in a PPP, within their own domain. Each entity should be responsible for the data they own. National authorities should ensure that monitoring is in place on important information exchange points. The monitoring performed by authorities, together with information provided by the network operators, will provide the needed national overview.	__
49.	Vodafone	Yes, it may be developed to address specific concerns that may arise.	However, a principle based approach should be adopted at present. A requirement for publishing of a Data Protection, Security and Privacy Policy in the public domain/on its website, should be prescribed. 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.	FCSO	—	—	—
51.	CUTS	—	—	—
52.	CGS	Yes, the latest technological innovations should be integrated and adopted to enable the Government and its agencies to effectively monitor data privacy and security systems of every entity handling personal and private data.	—	—
53.	CPA	Yes.	—	—