TABULAR MAPPING OF STAKEHOLDERS' RESPONSES TO QUESTION 12 - TRAI CONSULTATION PAPER: CROSS BORDER DATA FLOWS

The following table was prepared after an analysis of all fifty-three (53) responses to the "*measures that can be considered in order to address the potential issues arising from cross border flow of information and jurisdictional challenges in the digital ecosystem?"* under question 12 of the Consultation Paper. 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 chapters 8 and 9 of the White Paper, namely, the concerns related to rights of the data subject, foreign surveillance, law enforcement, and impact on the economy, development and innovation.

Sl. No.	Stakeholder	Comments/recommendations on regulatory approaches	Issues Addressed			
			Rights of the data subject	Foreign surveillance	Law enforcement	Impact on the economy, development and innovation

1	IAM AI	The Indian government should have access to data generated in India even if stored abroad. India should become a member of multi-party agreements. The data protection framework should not create unnecessary barriers to cross-border information flow, including administrative and technology restrictions for businesses. 1. Countries should develop frameworks where they mutually recognize cross border privacy rules.	—	—	—	Unreasonable data restrictions will deprive Indians of simultaneous access to the world's best technology and products. This is important particularly in the

						context of a cashless and digital economy. India becoming a member of multi-party agreements will help Indian (especially IT) companies get more market access.
2	ACTO	Regulatory frameworks should avoid and eliminate barriers to cross border data flows (CBDF).	Consumers have a	—	—	CBDF essential for global

		Consistent and predictable privacy protections are needed for consumers, irrespective of nature of data sharing. Empirical evidence of specific harm must determine contours of policy. Policy must be technology neutral and future proof. Governments must use Mutual Legal Assistance Treaties (MLATs) and other established processes to request and share data with each other.	rightful expectation of privacy and security of their data.			digital economy. Different sectors including services, manufacturing, agriculture rely on digital communication and other data transfers. CBDF have led to the emergence of global value chains where businesses' operations are

						spread across borders, increasing efficiency, lowering costs and quickening production.
3	ASSOCHAM	Jurisdictional issues must be addressed by building government consensus through cooperative mechanisms. Some countries are already cooperating on information sharing and cyber security and have entered into agreements for the same.	—	—	—	Disrupting CBDF will harm innovation, cut off India from the global digital value chain, and, the economy will not be able to compete globally with

						other economies.
4	COAI	Unified Licence Agreements (ULA) already mandates data localization of user identifiable information. However, transfer of information by users through handsets/websites defeats the point of the mandate. Law enforcement agencies should use MLATs for access to data stored in other jurisdictions. They must also draw up new robust ones, and amend existing ones to add provisions for lawful interception or access to data on the cloud.	__	__	__	The evolution of the volume and characteristics of data flow might result in higher risks for individuals, but companies generate economic value out of data by information collection and advanced analytics.
5	GSM	Regulatory framework for CBDF should be interoperable	__	__	CBDF must be	Regulatory

	A	which will create legal certainty, allowing companies to build scalable/robust data protection frameworks. Regulatory framework must take into account practical experiences, challenges and potential of a global, interconnected economy. The current framework is confusing and conflicting – it is a patchwork of international, regional and national law. Asian Pacific Economic Co-operation's (APEC) Cross-Border Privacy Rules are a good example as they facilitate CBDF while also seeking to achieve genuine and consistent standards of privacy protection across the region. Regulations must be clear.			restricted only in exceptional circumstances such as threats to clearly defined national security issues, to be assessed on a case by case basis.	environment must support both local and international investment. This will help local players grow and builds international business collaborations.
6	ISPAI	Issues around CBDF may be resolved through bilateral agreements between government and global associations. All entities providing a service in a country should be subject to the data security laws of that country. Certain kinds of data including financial/critical infrastructure related data may be localized.	—	—	CBDF create jurisdictional challenges for authorities while they might be used for	—

		Data protection/data security laws should apply horizontally, and be technology/platform neutral..			monitoring national security requirements.	
7	NLUD	—	—	—	—	—
8	Spantechnologies	Large tech multinational companies (MNCs) must be told to localize data of most widely used services in order to ensure individual privacy and data security. Localization Additionally, costs of international traffic will not have to be incurred since most net traffic to these sites will work within national borders. Possible role of NIXI in "aggregating such national traffic" is highlighted as important. India needs to build a national infrastructure to implement strong privacy regulations and protect itself against domestic and international cyber attacks.	—	—	Localization should be mandatory; It will be good for law enforcementas it will ensure that the government can monitor services (of large tech MNCs and others) for compliance with	By laying emphasis on data security and user privacy, service providers must generate trust/confidence with their clients such that it leads to an increased use of secure services.

					Indian laws.	This will in turn result in innovation, employment and economic growth. Regulations should not hinder future innovation.
9	TRA	__	__	__	__	__
10	NASSCOM - DSCI	Governments should work with each other in multi/pluri/bi-lateral fora to find solutions to extra terrestrial data access by law enforcement. India must lead and ensure that its issues are addressed. For example, we can lobby to be categorized as a country that meets the adequacy requirement. Partners should be identified for submitting and discussing the identified issues and approaches / recommendations.	Identified as a concern because of which countries are worried about			Localization adversely affects exports, may deter companies from undertaking cross border business, may

		For e.g. WTO, WITSA, EU, DPAs, FTC, etc India should reconsider and revaluate Budapest Conventions pros and cons, and whether it should result in something meaningful if India were to become signatory to it.	CBDF.			threaten innovation, threatens open architecture of the internet, hurts international competitiveness, results in less choice for the consumer with higher prices. Similar measures by other countries will severely harm India's IT-BPM industry, a major

						contributor to India's GDP. App developers need unfettered data flows. Smaller businesses lack resources to build/maintain infrastructure in every country of business.
11	ACT	—	—	—	—	TRAI's privacy rules must unambiguously allow CBDF.
12	Zeotap India	Private parties must have the option to use contractual/technical safeguards including standard contractual clauses and binding corporate rules to	—	—	—	—

	Pvt. Ltd.	overcome international data transfer restrictions. India must ask the EU for an equivalent of the Privacy Shield so that Indian companies have access to EU data.				
13	Takshashila Institution	Data controllers with an Indian presence must be answerable for violations in India. It is likely that this will result in companies entering into contracts with their foreign counterparts to share any potential liability. Indian citizens' data should be protected under the data protection framework.	itizens must always have a cause of action in India.	—	—	—
14	ISACA	Possible measures that focus on the cross-border flow of information merit further examination. The measures could include General Data Protection Regulation (GDPR) and Privacy Shield.	Inform the individual as to what informatio n is collected during the	—	—	—

			cross-border flows and the potential threats/risks to privacy.			
15	IBM	__	__	__	__	__
16	Make My Trip	Data collectors should only share data with reliable processors with reasonable systems in place to ensure data security. Data must only be used for specified purpose.	The user should exercise control over their data, its usage and sharing.	__	__	CBDF is very important for growth of Indian business.
17	Access Now	Outside the scope of TRAI.	__	__	__	__

		Past work on MLATs is linked.				
18	USISPF	Companies have invested a lot of money in ensuring the security of their data centers. Having servers at multiple locations is an asset – in case of a natural disaster or technical failure in one data center, another can take over and ensure uninterrupted service. Local data storage is also more vulnerable to cyber-attacks since it is harder to implement latest security software updates.	—	—	—	Any disruption to CBDF will adversely impact innovation, economic competitiveness, availability of new tech/services to users. Small businesses and startups rely on cloud computing given its affordability.

						Cloud computing works because of large economies of scale and globally distributed data centers.
19	ITI	Applying privacy laws extraterritorially conflicts with the global nature of the internet, raises conflict of laws issues. Conflict of laws along with data localization will hinder the creation of global privacy norms and increase compliance related challenges. There should be no data localization requirements. Data protection laws should be limited to (a) territorial application to organizations established within country or (b) organizations that deal with resident data subjects.	Protect rights of data subjects resident in a country under that country's data protection	—	Use MLATs and other arrangements to achieve law enforcement and counter terrorism objectives.	Data localization and extra territorial application of privacy laws will restrict growth and is bad for the global market.

		India should work on making MLATs and other arrangements more effective.	laws.			CBDF and adequate privacy safeguards are not mutually exclusive. India should identify and use existing frameworks that meet both objectives.
20	Sigfox	No data localization. India must use and work towards expanding MLATs and other cross border data request mechanisms. India should leverage existing multilateral agreements including the Budapest Convention on Cybercrime. The scope of such agreements should be "sensible". They must	—	—	—	Data localization harms innovation, productivity, growth for local and global

		(a) extend to organizations established in a particular country; and (b) to resident data subjects.				companies, both. CBDF and privacy/data protection are equally important and the law should balance both.
21	Exotel Techcom Pvt. Ltd.	India should sign treaties with countries where the most/large data servers are located and ensure that Indian law will apply for the data of Indian users. For data held in the cloud, when there is a "real and substantial connection" with India – India should have jurisdiction. "Real and substantial connection" means (a) data of Indian residents or (b) collected, stored or processed in India (c) foreign entity present in Indian in	—	—	—	Cloud computing is based on sharing servers. Many factors determine the server location, including seismic safe

		any form – agent/branch office/subsidiary etc. (d) if the services of the foreign data collector affect commerce in India.				zones and the size of the market. CBDF inevitable.
22	KOAN	Don't impose data localization requirements (if any) only on the ground of protectionism. Identify countries with high volumes of Indian data flows and address jurisdictional challenges through negotiations, mutual recognition and acceptance instruments. US-EU Privacy Shield cited as a good example.	—	—	—	CBDF is essential for international trade, for essential services (including cloud computing) to companies around the world. These services need and work on globally

						distributed servers. Unreasonable restrictions on CBDF are bad for India as we'll lose out on simultaneous access to the world's best technologies/products, international competitiveness.
23	IFF	This issue may be outside of TRAI's mandate. Rules and this issue are complex and therefore an expert	—	—	—	—

		body is needed to ensure certifications of other countries.				
24	Mozilla Corporation	Data localization is bad. Focus on reforming the MLATs that India is a party to as these are well established tools but are often slow and cannot keep up with speed of data transfers. Reform MLATs to improve their efficiency – (a) authenticate law enforcement requests and court documents through (perhaps) a centralized system (b) put in place a simple, consistent method for submitting requests online – could be either centralized or country specific, or even company specific (c) international standard format for companies to use while turning in evidence (d) single points of contact within governments and companies. Adopting GDPR level/"adequate" level of data protection will lead to several benefits including investment in India	—	—	—	Data localization threatens the growth of the internet and internet based services, increases costs and limitations on innovation, and, development and use of technology. Different data protection standards in EU

		and access to the EU/other foreign markets for Indian companies.				and India increase compliance costs (including capital and HR) for Indian businesses with global ambitions. It will hamper innovation, development and cause foreign companies/investors to rethink investing in India.
25	IDP	TRAI should be concerned with CBDF only in so far as	__	__	__	__

		foreign telcos are dealing with data of Indian citizens. Such telcos should be required to comply with India's data protection framework. TRAI should not deal with content and service providers handling user data.				
26	Citibank	The proposed Indian Telecom regulatory framework should regulate the transfer of personal data to other countries that do not ensure an adequate level of protection to privacy rights. Such obligations need to be imposed on the data controllers that engage in cross-border flow of information.	—	—	—	—
27	iSPIRT	Indian rules and regulations should apply to all regulated entities handling any data of an Indian user, including when the data or servers are not physically present in India. When such data leaves India, the authority must be notified, generally not on a per use basis, but based on the situation.	Indian law may apply extraterritorially to protect data of Indian users.	—	—	—
28	CIS	MLATs process need to be reformed as,currently, delays	Where	—	CBDF may be	CBDF is

		are hindering the law enforcement process. MLAT's may be formulated in accordance with the principle of "Safeguards for International Cooperation". Explore model contracts, data adequacy, binding corporate rules (BCR) for interoperability and preserving privacy while also facilitating trade. Data Protection Authorities (DPAs) across jurisdictions can enter into arrangements with each other to cooperate while implementing privacy laws. Existence of a DPA will allow a country (India) to be a part of and leverage international networks such as the Global Privacy Enforcement Network.	laws of more than one country may apply to communication surveillance, ensure through MLATs/other treaties that the law which ensures a higher standard of protection		vital for law enforcement authorities around the world to exchange information/intelligence etc.	imperative for innovation, performing business activities such as supply chain monitoring/delivery and picking up tracking etc.

			for the individual is applied.			
29	USIBC	Data localization is not good. Country level "adequacy" is inconsistent, problematic and deters innovation and following this approach make it hard for India to interact with the global, digital economy, deprive citizens of cutting edge services and products that they seek, and expose it to a global security risk. Model contracts and clauses, BCR, global corporate standards, standard contractual clauses are widely accepted and will help India seamlessly integrate with the global digital economy. APECs Cross Border Privacy Rules (CBPR) system is a good model. .	—	—	—	CBDF essential for modern economy and for societal progress. India's privacy framework should be interoperable with global practices as this will enable innovative and dynamic digital economy.

30	Disney Broadcasting (India) Ltd	—	—	—	—	—
31	BSA	Law should ban data localization for public and private sectors both. The OECD established accountability model, integrated into many legal systems is a good approach to cross border data governance. APEC CBPR is also a useful model for India to reference.	—	—	—	Data localization harms the implementation of security measures, impedes innovation and reduces services available to consumers.

						CBDF critical for cloud computing, data analytics, other emerging technologies.
32	ITfC	India should asset national rights over its data. This will put India in a better position to negotiate global agreements about data flows. New agreements based on national ownership of data only mean a just and fair global economy and data flows and not that data systems have become territorialized.	Data collected from Indians is a collective national resource and must be treated as such. This is the first step in solving the	If foreign countries have access to Indians' data, they will be able to exercise economic, cultural, social and	—	—

			problem of "data and digital intelligence" of every sector being "hoarded" abroad.	political control over the country.		

33	SFLC	Companies should be allowed to transfer personal data out of India only to countries with comparable data protection standards to ensure that companies do not use cross border transfers to violate privacy rights. In this context, cross border data transfer mechanisms under the GDPR including, but not limited to, the adequacy framework, binding corporate rules and standard data protection contractual clauses are instructive. Indian laws/jurisdiction should operate over website or service which targets Indians. A website or a service may be determined to be targeting Indians if it: (a) uses an Indian language (b) allows users to enter an Indian address (c) mentions India, Bharat or Hindustan prominently (d) allows payment through Indian rupees (e) has a registered office in India. In addition, body corporate that cater to Indians may be mandated to have a data protection officer who has to be located in India, subject to the body corporate satisfying	—	—	Exercise of jurisdiction under the laws of India may be enforced by mandating that the local agents of a body corporate, incorporated outside India, is liable for the acts of the body corporate.	—

		other conditions including a minimum threshold of number of employees or revenue turnover. If such website or service does not obey Indian laws and there is no way to enforce Indian laws, then it may be prevented from operating in India or targeting Indian users.				
34	EBG	Data localization is bad for many reasons.	—	—	—	Small businesses and startups need cloud computing. Cloud computing relies on

						economies of scale with globally distributed data centres. Cite a 2014 ECIPE study to highlight significant economic losses for India including a drop in the GDP. Data localization is bad for the IT industry, hurts innovation, economic

						competitiveness and the availability of technology and services to users.
35	AT&T Global Network Services India Pvt. Ltd.	Do not impose data localization as it will have harmful effects. Use MLATs and similar processes. Update existing MLATs to cover communications associated with evolving networks and services. APEC CBPR, Privacy Shield and EU-US Principles of ICT Services are good examples/models.	—	—	—	CBDF essential to global digital economy. Data transfer mechanisms should be predictable and interoperable. Imposition of data localization measures may

						see other(outsourcing) countries reciprocate, which will hurt the Indian economy and employment.
36	BIF	Forced localization is not recommended, rather, a regulatory framework for international data transfers that sets adequate guarantees to users' data but does not restrict or prohibit the data flows from the outset. It must be technologically neutral and interoperable with international standards. CBDFs are subject to international trade laws and norms, the main ones being non-discrimination and transparency. All major international data protection instruments recognize the need to facilitate the free flow of data, including personal data.	Access to information is an international human right.	Forced localization does not create safeguards against foreign surveillance as storing data in	Restrictions on cross border flow of data may be permitted for the purpose of ensuring national security. MLATs need to be made more effective. The law enforcement	Disrupting CBDFs is bad for innovation, economic competitiveness, and availability of technology and services to users. The 2014 ECIPE study

		Cross regional instruments like the APEC CBPR based on mutual recognition of privacy norms by members countries should be preferred over unilateral adequacy models as they enable cross border data flow without additional administrative burden. Contractual freedom should be preserved provided the privacy protections are applied in the contractual arrangements. Prescribing templates for the same would amount to regulatory overreach. New bilateral and multilateral agreements must be created, outside the framework of MLATs which would allow foreign companies to respond to requests by Indian law enforcement agencies.		one location could create a more attractive target.	requests for digital evidence should be linked to the location and nationality of the users, as opposed to the location of the data.. In addition, bilateral agreements on the lines of UK-US agreement should be encouraged between India and other countries	estimated that India's GDP would slump by -0.8% if an economy wide if an economy wide data localisation measure were introduced. Startups and small businesses rely on cloud computing. In addition, the Indian IT/BPO sector which is the world's

						largest sourcing destination for the IT industry will suffer and also place it at a competitive disadvantage with others in the APAC region. Rules based on the principle of reciprocity facilitate access of companies to new or restricted markets.
37	Sange	Personal sensitive data of Indians should not be allowed to	Fundament	Personal	__	__

	et Sindan	be transferred outside India. Data controllers must be subject to specific conditions before they can transfer personal data especially in the case of banking, insurance and fintech sectors.	al rights of a data subject could be undermined in cases where her personal data is disclosed as a result of arbitrary compulsion by a foreign country.	data of Indian residents transferred/ stored in an enemy/hostile country, the security of this data would be under threat.		
38	Redmorph	—	—	—	—	—

39	Baijayant Jay Panda	Different countries that we interact with should have similar data protection norms as ours to uphold data security.	—	—	—	CBDF must be strictly monitored, but are very important for data companies to thrive, in our current techno-digital ecosystem.
40	Apurv Jain	CBDF should take place only to countries with adequate levels of protection. Adequacy should be assessed based on all circumstances surrounding the transfer including (a) nature of personal data (b) purpose of processing (c) duration of processing (d) country of origin (e) country of final destination (f) rule of law (g) professional rules and security measures. A commission must be setup to evaluate cross border data	—	—	—	—

		transfer requests. Commission will approve if it deems country to be adequate. Commission in addition to the above factors must consider human rights and freedoms, existence and effective functioning of data protection agreements and international commitments on personal data protection. Adequacy status of countries may be revoked. BCR is also a good mechanism for CBDF if they meet GDPR requirements.				
41	RJIL	Adopt a data localization approach – many other countries are doing so already. Any movement abroad should undergo security assessment. China's Counter Terrorism Law requires internet and telecom companies and other critical infrastructure service providers to localize data in China and also provide encryption keys to government authorities. Indonesia introduced general data localization requirements (data center and disaster recovery center in	Sensitive data of Indian citizens should be processed and stored in servers within India's	—	—	—

		Indonesia) relating to data for public services. See Article 1 of the Draft Ministerial Regulation concerning Data Center Technical Guidelines. See also Article 17(2) of the Regulation on Electronic System and Transaction Operation in Indonesia which mandates data localization for law enforcement, protecting citizens and sovereignty of state. Russia introduced data localization in September 2015 – personal data of Russian citizens should be stored in servers in Russia. Transition provision for large foreign MNCs to allow time to comply with this law. South Africa forbids CBDF unless they satisfy certain requirements including comparable level of privacy protection. Canada's British Columbia and Nova Scotia mandate personal data held by public bodies including schools hospitals and public agencies should be stored and accessed only in Canada – there are some minor	geographical boundaries.			

		exceptions. UK – data controllers must register with the Information Commissioner to report intention to process personal data before beginning. Have to pay fees, and renew annually. Data Protection Act allows a limited transfer of data to non–EU countries, subject to many conditions.				
42	Bharti Airtel Limited	All entities providing communication related services must be subject to the same rules which must be technology and platform neutral. Example Currently, telecom service providers have the obligation to data localize, but not others dealing with the same data. Jurisdictional issues in the digital ecosystem should be addressed through bilateral agreements between the Government and other global associations such as the United Nations Organization (UNO). Entities sending the consumer data abroad and the foreign entity handling the data should be subjected to Indian laws related to privacy and data protection.	—	Certain data such as biometrics, critical infrastructure data, financial transactions data may be localized in the	—	—

				interests of national security and public interest.		
43	Idea Cellular Ltd.	The information of Indian customers held by global companies operating in India, that have their data servers located in their country of incorporation, should be mandated to be handled in a safe, secure manner. Such companies should also be subject to audit by relevant authorities. Direct global companies manufacturing mobile devices in India to disclose details of the procedures and processes	—	—	TRAI's recommendation cloud computing to address the issue of access to data, that is hosted by cloud service providers	—

		followed by such companies to safeguard security of data in their products. Artificial Intelligence and Machine Learning enabled architecture should be implemented by the Government to intercept and analyze any cross border data exchange.			in different jurisdictions, by law enforcement agencies may be considered in respect of jurisdictional challenges pertaining to cross border flow of information in the digital ecosystem, i.e.,: Robust MLATs should be drawn up with jurisdictions where CSPs	

					usually host their services, enabling access to data by law enforcement agencies Existing MLATs should be amended to include provisions for lawful interception or access to data on the cloud..	
44	MTNL	Exercise of jurisdiction by a court of law, that forms the very basis of any justice delivery system, is challenged by the internet. The Information Technology Act, 2000 provides for extra territorial jurisdiction, subject to	—	—	—	—

		satisfaction of conditions provided under the Act. The principles applicable in case of cyber crimes should be made applicable to the present issue.				
45	Reliance Communications Ltd.	Security requirements for digital service should be a combination of security measures enunciated for the telecom domain, IT domain as well as the cloud computing domain. Data localization is recommended to address the challenges arising out of CBDFs. For addressing the jurisdictional challenges local hosting of users personal data, especially by the data collectors, should be mandated. India should enter into MLATs with other countries as MLATs help to obtain information from data controllers that host data outside the territory of India. Assistance may be denied by either country (according to agreement details) for political or security reasons, or if the criminal offence in question is not equally punishable in both countries.	__	__	Mandatory data localization has ensured sufficient support for law enforcement agencies.	__
46	TTL	__	__	__	__	__
47	BSNL	Major content providers' data should be hosted within the	__	__	__	The

		country.				government agencies have need to come up with a balanced solution to address the twin concerns of threats to personal privacy by the more intensive use of personal data and the risk to the global economy of restrictions on the flow of information.

48	Telenor	Regulations designed to protect consumer data should be applied regardless of industry or service offering. Challenges to enforcing data protection requirements for those business models without a physical presence in the region are addressed by the GDPR: a. Any transfer of personal data for processing should take place only after complying with GDPR provisions. b. Personal data should be transferred only after ensuring adequate level of protection. c. Personal data should be transferred only after ensuring availability of appropriate safeguards – rights and legal remedies to data subjects. d. Binding corporate rules should be in place before any transfers. e. International cooperation should be pursued for protection of personal data.	—	—	Requirements like that found in the GDPR not only apply to players in the digital ecosystem but to all data controllers and have an extra-territorial effect for compliance and violations.	Global competition requires countries to facilitate CBDFs.
49	Vodafone	Collaborative regulations are needed for digital societies as borders are vanishing and becoming irrelevant. Light	—	—	TRAI's recent recommendation	Digital economies and

		touch regulations are recommended Any restriction on cross border flows is archaic in the era of globalization and cloud computing. Information must be allowed to freely flow across borders. Data controllers should be made responsible to ensure that the data subject is assured of the same level of protection that is applicable in their own country.			s on access to data hosted by cloud service providers in different jurisdictions, by law enforcement agencies, are relevant in addressing jurisdictional challenges. In particular, TRAI recommended effective MLATs with jurisdictions where cloud service providers	innovation need light touch regulation to thrive.

					host their data and amendment of existing MLATs to provide for lawful interception and access to data in the cloud.	
50	FCSO	Suggestions by Justice A.P. Shah Committee were recommended for consideration.	—	—	—	—
51	CUTS	Enhanced inter-governmental cooperation must be pursued to pave the way ahead for cross-border data flow to accelerate the growth of digital trade, without compromising on the data security and sovereignty, and ensuring fair competition in the market.	—	—	—	Free flow of data helps micro, small and medium enterprises reach customers across the globe

						and participate in global value chains. It is recommended that privacy rights are safeguarded without restricting trade.
52	CGS	There should be proper consultation and co-ordination among Telecom and other sectoral regulators across the World for facilitating effective regulation over cross border flow of information Multilateral agreements among nations is recommended to address jurisdictional challenges, concerns arising out of cross-border flow of information and issues of related to effective compliance of data protection and privacy regulations. The international best practices on cybersecurity and	—	—	—	—

		data security should be studied and emulated. The jurisdiction of the regulatory Authorities should be extended to cover the personal data of users in India that is stored outside India by different service providers to effectively address the challenges arising out of cross border flow of information.				
53	CPA	Digital sovereignty can be safeguarded through various measures including strong national intermediary liability regimes, requirements to open local offices, demanding backdoors to encryption technologies and the imposition of full-fledged licensing regimes. Issue-based multi stakeholder policy networks must be created to develop scalable solutions. Draft legislations should include clauses establishing extraterritorial reach. The data of national citizens processed by foreign companies needs to be stored locally like Russia. Any national policy measure that would be detrimental if	—	—	—	—

		generalized around the world should not be adopted. Based on the lessons of the Internet & Jurisdiction Project, some key factors for the success of such issue-based policy networks are: • Framing the problem as an issue of common concern for all service providers. • Ensuring the neutrality of the convener and facilitation team/secretariat; • Involving all stakeholder groups: internet platforms, technical operators, academia, consumer advocacy groups, and international organizations. • Constructing and expanding a global network of key actors; • Creating trust among heterogeneous actors and adopting a shared vernacular; • Combining smaller working groups and reporting on progress to make the process manageable and transparent; • Informing stakeholders about relevant trends around the world to foster evidence-based policy innovation; and				

		• Providing sufficient geographic diversity from the onset to allow the scalability of adoption of any emerging policy solution. • Addressing jurisdictional issues on the internet and pre-empting the current legal arms race requires enhanced efforts to catalyze multi-stakeholder cooperation on the specific topics of cross-border requests for domain seizures, content takedowns, and access to user data.				