TABULAR MAPPING OF STAKEHOLDERS' RESPONSES TO THE WHITE PAPER ON A DATA PROTECTION FRAMEWORK FOR INDIA.

PART II - SCOPE AND EXEMPTIONS

The following table was prepared after an analysis of all twenty seven (27) responses to questions in Chapter 1 and Chapter 2 of Part II of the White Paper on a Data Protection Framework for India: - What are your views on what the territorial scope and the extra-territorial application of a data protection law in India should be? What measures should be incorporated in the law to ensure effective compliance by foreign entities inter alia when adverse orders (civil or criminal) are issued against them? What are your views on the issues relating to applicability of a data protection law in India in relation to (i) natural/juristic persons; (ii) public and private sector; and (iii) retrospective application of such law? Should the law provide for a time period within which all regulated entities will have to comply with the provisions of the data protection law? Are there any other views relating to the above concepts?

The table identifies the responses and suggestions of the stakeholders to the questions.

Stakeholders	Views on territorial scope and extra-territorial application of data protection law in India	Measures to be incorporated in the law to ensure effective compliance by foreign entities	Applicability of a data protection law in India in relation to (i) natural/juristic persons; (ii) public and private sector; and (iii) retrospective application of such law	Time period within which all regulated entities will have to comply with the provisions of the data protection law	Any other views

Industry Associations –3* BSA, iSPIRT, and ITI	**BSA**	Limit the scope of law to Indian residents, where personal data is collected from data subjects by an entity established in India which would ensure effective level of activity or subject to India law by virtue of international public law.	No response.	India's data protection law should apply only to natural persons.	No specific transition period suggested, however it is noted that in other jurisdictions, legislators have allowed a two-year transition period.	No response.

	iSPIRT	Law should revolve around the person, their data and the privacy concerns. It should be applicable entirely to the data of Indian residents that are processed by entities who do not have any presence in India.	Allow for escalation clauses that restricts market access and treaties (bilateral or multilateral) for redressal.	Law should protect data relating to natural persons and juristic persons. It must uniformly apply to public and private sector as well as the government. Implementation of the law should be in a phased manner where public awareness precedes penalties. It must specify how the data collected in the past shall be dealt with in the future.	Sector-specific time period should be provided for the compliance.	Law must provide for private remedies against deliberate attacks on individuals or entity. Under the new law public clarification would harmonize how the data is collected by public and private authorities.

	ITI	Policymakers should forgo data localization measures and establish laws with territorial scope applicable to entities/data subjects established or residing in a certain country.	India should invest more in cross-border data request mechanisms for law enforcement and counter-terrorism purposes, including making Mutual Legal Assistance Treaties (MLATs) more effective tools for cross-border investigations and leverage existing multilateral agreements.	Retrospective application of the legislation could create huge burdens on businesses for both in Indian and international. As it would impact the countless contracts already signed by companies in addition to any new ones.	Government should provide reasonable timeframes, for organizations to prioritize and achieve compliance with the new law in all aspects of their business.	No response.

Civil society organizations – 12** 1. Access Now; 2. CCG; 3. CIS; 4. Centre for Trade and Investment Law; 5. Harvard FXB Center; 6. IDP; 7. Mozilla Foundation 8. ORF; 9. Professor Graham Greenleaf; 10. SFLC; 11. Legal	**Access Now**	Jurisdictional scope of the law should not be from an "establishment" perspective (where the entity is located) but from a user's perspective (where the user is located and where the user is from). It should indicate its extraterritorial application (i.e., to which actors, with what enforcement mechanisms) and provide users, companies, and authorities with clear avenues for remedies.	The law must give priority to the user over the interests of the state with respect to extraterritorial applications.	All public and private entities should be subject to the data protection framework and the corresponding authority emanating from such framework. No blanket exceptions should be made in application of law with respect to any entity.	No response.	No response.

Academics and Advocates; 12. Takshashila Institution.	**CCG**	Data protection law must have extraterritorial applicability. When it has, or is expected to have, some impact on, or effect in, or consequences for: 1) the territory of India, or any part of India; or 2) the interests, welfare or security of inhabitants of India, and Indians.	No response.	The law needs to apply to natural and juristic persons and public or private entities, who engage in the collection or use of data.	No response.	No response.

	CIS	The law must be applicable to India entirely and to any offence or contravention committed outside India by any person, if it is related to the personally identifiable information of an Indian resident. It should therefore be applicable to: - 1) entities in India, 2) entities carrying out business in India, and 3) entities providing services to Indian residents.	Entering into more Mutual Legal Assistance Treaties (MLATs) with countries will ensure that India has the capability to protect its resident's data.	Law shouldn't apply to juristic persons as personal data exists only for natural persons. Both public and private bodies are subject to the law. It can be retrospective in respect of the continued processing of data, but not to the extent that may require re-obtaining of consent.	In absence of any data protection guidelines, certain provisions such as notice, consent, opt-out, purpose specification and use limitation, data security, access/rectification, accountability, transparency, limits on third party disclosure needs to be implemented immediately. One year time period might be required for other provisions such as anonymisation and pseudonymisation, data localisation, data portability, creation of co-regulatory bodies, creation of standards and methodologies on data protection impact assessment and audits	No response.

					by DPA. Two year time period should be given for provisions like creation of standards and methodologies on data protection impact assessments, audits by sectoral bodies, drafts on sectoral codes and right to explanation. It is also proposed that breaches of regulation in the interim period could be addressed through corrective measures for one year rather than exercising the punitive measures.	

	Centre for Trade and Investment Law	No response.	No response.	No response.	No response.	No response.
	Harvard FXB Center	Law be applicable on an entity which does not have a presence in India but offers goods or services to Indian residents over the Internet, or carries on business in India or processes personal data of Indian residents, irrespective of its location.	A warning in writing should be placed in cases of first unintentional non-compliance with the law. Measures such as regular periodic data protection audits, monetary penalty, restricting market access, holding the Indian subsidiary/related entity liable for civil penalties or damages, are also proposed.	Laws that are applicable to natural persons, may extend to juristic persons. Law must apply to health data held by public and private entities. Also the law may have a transitory provision to address the issue of retrospective application.	No specific time period mentioned.	There should be periodic review of the adequacy or limits of exemptions granted, to ensure that the policy has kept up with evolving technology, and cultural acceptance.

	IDP	Entities based outside the country but offering goods and services to Indian residents, or monitoring their behavior should also fall within the scope of the data protection law.	No response.	The framework should be applicable to data of natural persons only. The law should apply retrospectively where the scale of data collection and processing exceeds a certain threshold.	A transition period should be allowed for, where the entities that have already collected data can comply with the requirements of the new law.	No response.

	Mozilla Foundation	It is suggested that India should adopt a GDPR-like model and other mechanisms for regulating entities which offer goods or services in India even though they may not have a presence in India.	No response.	No response.	No response.	No response.
	ORF	No response.	No response.	No response.	No response.	No response.

	Professor Graham Greenleaf	Law should be applicable to entities offering goods and services in India or with an establishment in India. It should not be applicable simply because a website is accessible in India. The law should be applicable on entities which can process 'personal data' of Indian citizens or 'residents' no matter where they are located.	No response.	The law should be applicable to natural persons only and not to deceased persons. Law must apply 'retrospectively' to data collected prior to the date of the Act.	There is usually a period between enactment and enforcement of Act. Such time period should be sufficient for businesses and agencies to 'clean up' their records.	No response.

	SFLC	The law should apply to State entities and private companies, partnerships or any other body corporate which functions within India through a registered place of business or establishment irrespective of whether data processing is carried at or outside India. It should also be applicable to entities which do not have a registered place of business or establishment in India and offer goods or services to persons in India, irrespective of consideration.	Local agents of body corporate can be held liable. Each body corporate of specified size, which targets Indian citizens, should have a data protection officer located in India. Entities can be restricted from accessing the market temporarily if they do not have a registered office in India and fail to comply with adverse orders.	Law should be applicable only to natural persons. It must be applicable to both public and private sector.	The law should allow a transition period for entities to bring their data processing practices in line with the requirements of the new law.	No response

	Legal academics and advocates	It is suggested that the regulation should have an extra-territorial effect. It should apply to web services and platforms which are accessible in India and which gather personal data of Indian citizens.	To ensure compliance, the data protection authority should be empowered sufficiently to confer adequacy status, to foreign countries from which such global platforms carry out their operations.	No response.	No response.	No response.

	Takshashila Institution	Law should protect Indian residents (regardless of their presence within or outside India when the data was processed) and foreign residents living and working in India but not to Indian citizens living and working in foreign countries. Accessing a website in India which does not target Indian residents, shall not require the operator of the website to comply with provisions of the law.	The data protection authority should have the ability to identify and hold accountable any foreign entity present in India, for compliance with any adverse orders.	Law must apply only to natural persons and not juristic persons. Law should be horizontally applicable to both government and public, and private sectors. The retrospective applicability of the law would impose significant and unwarranted challenges for entities collecting and processing data.	The law could incorporate a transition period to help regulated entities make changes to their data processing practices and ensure compliance with the new law. The time period would depend on the complexity of the transition.	No response.

Others- 12* ** 1. Anupam Saraph; 2. Bhandari, Kak, Parsheera, Rahman, and Sane; 3. DEF; 4. Dvara Research; 5. EFF; 6. EPIC; 7. IFF; 8. Omidyar Network; 9. Privacy International; 10. Subhasis Banerjee; 11. Suyash	**Anupam Saraph**	No response.	No response.	No response.	No response.	No response.
	Bhandari, Kak, Parsheera, Rahman, and Sane	Data protection law should extend to all sectors and entities that collect and process user data, whether in the public sector or the private sector. One-size-fits-all model is not recommended.	No response.	No response.	No response.	No response.
	DEF	No response.	No response.	No response.	No response.	No response.

Rai; 12. The Hoot.	**Dvara Research**	Foreign entities should be made subject to the law in circumstances where - 1) they conduct business in India, 2) process personal data from India or 3) process data for an Indian controller outside India.	No response.	The law should protect all natural persons (citizen and residents) present in India. It should also apply to private and public entities.	No response.	No response.
	EFF	No clear response.	No clear response.	No clear response.	No clear response.	No clear response.
	EPIC	No response.	No response.	No response.	No response.	No response.
	IFF	No response.	No response.	No response.	No response.	No response.

	Omidyar Network	Law should cover any entity processing the personal data of Indian residents. Territorial scope of a law should be determined by the need and capability to regulate. The law should also apply to entities that have no presence in India.	Measures such as restricting access to markets, penalties based on global turnover, mandatory establishing of a representative office and holding the Indian subsidiary/related entity liable for civil penalties or damages should be incorporated. The state should explore other means to hold foreign entities accountable.	No response.	No response.	No response.
	Privacy International	The law should apply to: 1) processing of personal data by entities established in India regardless of whether the processing takes place in India or not, 2) processing of personal data	No response.	The law should apply to natural persons only. It shall also apply to processing of personal data by both public and private entities.	No response.	No response.

		of individuals who are in India by entities not established in India, where the processing relates to: - a) offering goods or services to data subjects in India or b) monitoring their behavior within India.				
	Subhasis Banerjee	No response.	No response.	The same privacy protection principles cannot be horizontally applied to the state and other essential bureaucracies, for example banking and insurance, and to non-essential private digital services where user participation is voluntary.	No response.	No response.

	Suyash Rai	Jurisdiction issues could be: - 1) Territorial: It is difficult and expensive to establish jurisdiction over foreign organizations. It is suggested to begin with regulating entities that are already registered in India, and have offices here. 2) Sectoral: It is suggested that DPA should make regulations/standards in consultation with respective regulators, and once the regulations/standards are specified, the sectoral regulators should supervise and enforce the law and the regulations. 3) Based on organization type or size: it is strongly recommended to exempt small organizations from being subject to the data protection law.	No response.	Law should be applicable to both private and public sector. Small organizations should be exempt from the law.	No response.	No response.

	The Hoot	The data protection authority cannot have jurisdiction over the Indian media. Jurisdiction of the law should be limited to the government records.	No response.	No response.	No response.	No response.

***Industry Associations:** ITI – Information Technology Industry Council, BSA – Business Software Alliance, iSPIRT – Indian Software Product Industry Round Table.

****Civil Society Organisations:** Access Now; CCG – Centre for Communication Governance, NLU Delhi; CIS – The Centre for Internet and Society; Centre for Trade and Investment Law – Dr. James J. Nedumpara and Mr. Sandeep Thomas Chandy, Centre for Trade and Investment Law, Ministry of Commerce; Harvard FXB Center – Harvard FXB Center for Health and Human Rights; IDP – Internet Democracy Project; Mozilla Foundation; ORF – Observer Research Foundation; Professor Graham Greenleaf; SFLC – Software Freedom Law Centre; Legal Academics and Advocates – Submission by 24 Legal Academics and Advocates, and Takshashila Institution.

*****Others:** Anupam Saraph; Vrinda Bhandari- Advocate, Amba Kak- Mozilla Foundation, Smriti Parsheera, Faiza Rahman, and Renuka Sane- National Institute of Public Finance and Policy ; DEF- Digital Empowerment Foundation; Dvara Research; EFF- Electronic Frontier Foundation; EPIC- Electronic Privacy Information Centre; IFF- Internet Freedom Foundation; Omidyar Network-Subhashish Bhadra, Associate, Omidyar

Network ; Privacy International; Subhasis Banerjee- Computer Science and Engineering, IIT Delhi; Suyash Rai-Senior Consultant, National Institute of Public Finance and Policy; The Hoot- Prashant Reddy Thikkarvarapu.