RESPONSE TO WHITE PAPER ON DATA PROTECTION FRAMEWORK FOR INDIA

1. **Name: Baijayant Panda**
2. **Designation: Member of Parliament**
3. **Organisation: Independent**
4. **E – Mail address: office@bjpanda.org**
5. **Phone No.: (011) 2375 3430**

Baijayant 'Jay' Panda is currently serving his second term as a Member of Parliament in Lok Sabha. Previously, he has also served two terms in Rajya Sabha. Currently, he is a member of the Department-related Parliamentary Standing Committee on Home Affairs as well as the Consultative Committee for the Ministry of Finance and Corporate Affairs. Mr. Panda has previously authored and tabled a private member's Bill called 'The Data (Privacy and Protection) Bill, 2017.'

1. **Name: Samir Saran, Bedavyasa Mohanty, Madhulika Srikumar**
2. **Designation: Cyber Initiative**
3. **Organisation: Observer Research Foundation**
4. **E – Mail address: ssaran@orfonline.org**
5. **Mobile No.: +91 8130274172**

Set up in 1990, Observer Research Foundation (ORF) is a one of Asia's preeminent think tanks that provides non-partisan, independent analyses on matters of security, strategy, foreign policy and global governance. ORF's Cyber Initiative hosts CyFy: the India Conference on Technology, Security and Society. It also convenes Track 1.5 dialogues with the United States and the United Kingdom on cyber issues. ORF's research revolves around cross-border data sharing, security of digital payments, encryption and emerging technologies.

Introduction

Over November 18 and December 19, 2017, ORF convened two multistakeholder roundtables on data protection, chaired by Shri Baijayant Panda, to engage a wide range of stakeholders and solicit inputs on the various issues being considered by the Committee. The discussions at these roundtables presumed that technology driven innovation is only possible when individual data is safe and fundamental freedoms are protected. Experts from industry, civil society, academia and think tanks attended these roundtables (for list of participants see Annexure I) and considered various issues such as cross-border data sharing, data collection by communication service providers, law enforcement access to data and regulatory principles.

While the Committee has rightfully explored a wide gamut of issues that will be critical for privacy and security in the coming years, we have restricted our inputs to certain key questions. These issues represent what we consider are pivotal to the new data protection regime. The opinions expressed here, while encapsulating the conversations at the two roundtables, have been curated by ORF and the office of Shri Baijayant Panda, and do not represent the views of any particular participant in attendance.

Part No.: II- SCOPE AND EXEMPTIONS

Chapter No.: 7- Exemptions for Household purposes, journalistic and literary purposes and research

1. What are your views on including investigation and detection of crimes and national security as exemptions?

One of the most significant criticisms of the data protection rules under the Information Technology Act has been the limitation of its application to "body corporates." When law enforcement and intelligence organisations collect vast amounts of data, any broad

exemptions under the data protection rules would have the effect of nullifying their original intent. The data protection rules must specify practices around both access and storage of user data. Reasonable and granular exemptions must be provided for specific issues such as user notice, data preservation and specificity of target, device and account.

The white paper remains unclear on what form of exemptions are being considered for investigation of crimes and the purposes of national security. Any exemptions that allow the suspension of the right to privacy must be guided by principles of necessity, proportionality and transparency.

If exemptions are not narrow they leave open the possibility of non-targeted mass surveillance. Language currently employed by the Section 5(2) of the Telegraph Act, Section 26 (2) of the Indian Post Office Act and Section 69(B) of the Information Technology Act allows for interception of communications relating to "a class of persons" and "any subject matter." This form of ambiguity in legislative text causes a slippery slope where, through technologically advanced means, entire sections of the population can be brought under surveillance. Therefore, any exemptions for law enforcement access to data must only be allowed for interception requests that are targeted and have a clear, demonstrable nexus to a crime or threat to national security or public order. Similarly, the new law should not mandate or have the effect of allowing measures that can interfere with the technological integrity of devices and networks.

4. Should there be a review mechanism after processing information under this exemption? What should the review mechanism entail?

Yes, the new regime must prescribe a review mechanism after processing information for law enforcement and national security purposes. The current mechanism that exists under Rule 419-A(16) of the Indian Telegraph Rules, 1951 provides for the review of

interception orders passed under S.5(2) of the Indian Telegraph Act and S.69(B) of the Information Technology Act by a three member Review Committee. This committee consists of the Cabinet or Chief Secretary and two other secretaries of the centre or state government. The Rules mandate that the committee shall meet at least once every two months to examine that due process was followed in intercepting communications.

A recent application under the Right to Information Act to the Ministry of Home Affairs has revealed that on an average, 7500 to 9000 orders for interception are issued every month by the Central Government alone. Therefore, if the Review Committee meets once every two months (as it is statutorily mandated to do) then it would have to consider and dispose off between 15000 to 18000 orders of interception at every meeting. If, on the other hand, the Review Committee were to meet every day of the month it would have to dispose off between 290 to 345 orders.

This is clearly unsustainable. If the requests made for interception of communications and user data number in the thousands every month then the review of these orders must be undertaken by a permanent body or one that meets more frequently than once every two months. The constitution of the committee should also be modified to include a judicial member to test their compliance with the law and a technical member to assess whether adequate information about the subject of investigation could have been obtained through less intrusive means.

5. How can the enforcement mechanisms under the proposed law monitor/control processing of personal data under this exemption?

One of the primary problems with Indian surveillance law is the executive authorisation model for intercepting communications. Both surveillance and interception of one's communication are a restriction on one's fundamental rights. They can therefore only be undertaken with due regard to procedure established by law. Any restriction imposed

on the right to privacy must also be determined with regards to the particular facts and circumstances of a case. An order of surveillance can impinge upon the right to privacy and impose a chilling effect on free speech. Every such order must be tested against the limits set under Article 19 of the Constitution. This determination can only be done adequately by a judicial officer and not by an executive authority.

It is for this reason that almost all countries with specialised legislations for preventing unlawful surveillance have favoured a judicial sanction model over an executive authorisation one. In Australia for instance, warrants for intercepting communications are granted by a judge or a nominated member of the Administrative Appeals Tribunal. The Australian Telecommunications Interception and Access Act also clearly identifies which judges and nominated members are authorised to issue such warrants. In case of the nominated member, such member must have been enrolled as a legal practitioner of either a Supreme Court or a federal court for not less than five years. It is only in case of an application for interception by the Australian Security Intelligence Organisation that a warrant is not required from a judge or a nominated member. But even so, a warrant must be obtained from the Attorney General after judicial application of mind. In Brazil, wiretapping is regulated by the Federal Law No. 9,296. Under this law, authorisation for interception is granted on a Judge's order for a period of 15 days at a time. Moreover, interception is only allowed for investigations into serious offences like drug smuggling, corruption, murder and kidnapping. The Canadian Criminal Code, 1985 which governs general rules of criminal procedure including search and seizure protocols also favours the judicial sanction model. Under the Code, interception orders can only be issued by a provincial court judge or a judge of the superior court. Similarly, in the United States authorisation for interception can be granted by a district court or a federal appeals court on application by a law enforcement officer duly signed by the Attorney General. In France, the civilian law governing video surveillance and

interception of communication, also requires previous authorization from an investigating Judge after consultation with the Public Prosecutor. This reflects a clear lean in favour of letting the judiciary allow or disallow requests for interception of communications.

Of the countries that gained independence on a comparative time scale as India, only three have managed to draft specialised laws regulating interception. All three of these countries have opted for a judicial sanction model for intercepting communication. South Africa, having gained independence in 1931, drafted the Regulation of Interception of Communications and Provision of Communication-related Information Act in 2002. Under this law a warrant for intercepting communications and installing surveillance devices is granted by a designated judge. Such warrant is issued on satisfaction of the judge that the investigation relates to a serious offence or that the information gathering is vital to public health or safety, national security or compelling national economic interests. Cyprus, that gained independence in 1960, drafted the Protection of Secrecy of Private Communications (Call Interception) Law in 1996. Under this law, the Attorney General must file for a court order before using wiretaps. The latest among the three countries to have modernised its surveillance laws is Pakistan. There, the power of law enforcement and intelligence agencies to intercept communications and undertake covert surveillance is governed by the Investigation for Fair Trial Act, 2013. The Act provides for a two-tiered supervisory model for authorising interception. Under §6 of the Act, every application for interception must be placed before the Federal Minister for Interior for his due consideration. It is only with the Minister's permission that the application can then be placed before a High Court Judge for the issuance of a warrant.

The new data protection Bill, too must adopt a judicial sanction model for authorising access to communications and user data by law enforcement and State agencies.

6. Do we need to define obligations of law enforcement agencies to protect personal data in their possession?

The new law should define obligations for law enforcement during prevention, investigation and prosecution of criminal offences.

The Bill must recognise a distinction between preservation and retention of data by communication service providers for investigative purposes. Currently, under S. 67(c) of the IT Act data preservation and data retention are treated interchangeably. S.67(c), titled "Preservation and retention of information by intermediaries," imposes an obligation on intermediaries in India to retain information in a format, manner and for a duration as prescribed by the Central Government. Data retention, however, is different from preservation. Data preservation follows a specific request by a government agency to store data for a limited duration while the agency undergoes a legal process to compel the disclosure of the information. Data retention on the other hand requires companies to store all data for an unlimited amount of time in the event that the information is needed for an investigation.

While data preservation can often be necessary for ensuring that evidence is not lost or automatically deleted in the aftermath of a crime, data retention interferes with an individual's right to remove her personal information stored online and in conflict with the right to privacy.

Part No.: III Grounds of Processing, Obligation on Entities and Individual Rights.

Chapter No.: 1 Consent

1. What are your views on relying on consent as a primary ground for processing personal data?

Alternatives:

a. Consent will be the primary ground for processing.

b. Consent will be treated at par with other grounds for processing.

c. Consent may not be a ground for processing.

2. What should be the conditions for valid consent? Should specific requirements such as "unambiguous", "freely given" etc. as in the EU GDPR be imposed? Would mandating such requirements be excessively onerous?

3. How can consent fatigue and multiplicity of notices be avoided? Are there any legal or technology-driven solutions to this?

Informed and meaningful consent remains a foundational protection in collection of data. This consent must be freely and expressly obtained. This must be bolstered by purpose specification for collection, handling and transfer of data. The various interests that an individual's data will be used for must be clearly notified to a user. This consent must be simplified and multilingual. The consent must also be flexible allowing users the option to revoke access to their personal information at a subsequent time.

Every user must also have a right to retain a copy of her aggregated information and the right to erase copies of the information stored with the primary data controller. The law should require that the obligation to erase this data must be built into privacy policies of data controllers.

To address consent fatigue, the law should prescribe different 'grades' of data collection practices that all privacy policies must necessarily fall under. In addition to the text of privacy policies and data sharing practices, this gradation must be made prominently visible by the data controller. For services that employ privacy by design such as anonymisation of user data, special certifications can be granted by the regulator to incentivise their competitors. These grades can be assigned in the form of easily intelligible combination of letters and numbers, so that users can recall what type of data collection practice each privacy policy corresponds to. In a manner similar to

Creative Commons Licences, or ISO standards, privacy policies of different services can be categorised differently, depending on the nature of data they collect. This can help inform user choice when signing up for a particular service online.

The new data protection authority along with the industry should conduct technical analyses and determine which forms of data are necessary for which services. For instance, the data set required by apps providing banking services will be very different from apps providing health and fitness services. This is a necessary corollary of purpose limitation -- that can limit the collection of data that is not absolutely necessary, and therefore limit the harm that potential breaches or misuse can cause.

This is especially important in the context where individual informed consent is not adequate for anticipating future harms. For instance, machine learning collate aggregated data sets given for a certain purpose to make other more insidious inferences. This potential harm can be mitigated by limiting data collection in the first instance.

Part No.: II - SCOPE AND EXEMPTIONS

Chapter No.: 9- Data Localisation

1. What are your views on data localisation?

4. If the data protection law calls for localisation, what would be impact on industry and other sectors?

The White Paper correctly identifies the impetus for data localisation as prevention of foreign surveillance, protection of individual rights and easy access of data for law enforcement. While India can certainly demonstrate a need to store data locally, there are many operational difficulties for both the private sector and in public interest.

Data centres are extremely expensive to build and maintain. Most data centres also require very little manpower and most of the investment goes into acquisition of equipment. They will, therefore, not generate any substantial employment. The required infrastructure often cannot be manufactured locally and will have to be imported thus driving up costs. Most importantly though, data localisation can harm innovation among

startups that rely on cross-border data transfers. The architecture of the internet also does not a support fragmented and localised internet.

However, there are certain measures that can be considered to address India's data needs. For instance, to address concerns of foreign intelligence surveillance, data collected by public entities such as biometric data can be mandated to be stored on Indian soil. This will ensure that publicly held data, data relating to Critical Information Infrastructure in certain sensitive sectors etc. is not easily compromised. The Guidelines for Government Departments on Contractual Terms Related to Cloud Services issued by MEITY in March, 2017 are a good starting point in this regard.

Access to data for law enforcement currently takes place through a legacy law in the form of Section 91 of the Code of Criminal Procedure. For instance, to obtain non-content data from foreign companies and any data from Indian companies an investigating officer only produces a notice with no legally recognised format. This process not only lacks safeguards but also makes no distinction between sensitive and non-sensitive data. Given these realities, the data protection Bill should consider a complete overhaul of access to data, specifying different legal treatment for more sensitive data sets. Until such time, calls for data localisation may be premature.

At the same time, the Committee must recognise the need to build capacity among law enforcement agents to make requests for data stored abroad. Currently, requests for content data to foreign companies are made through either the Letters Rogatory or Mutual Legal Assistance Treaties which are time and resource intensive. The new data protection authority once established should explore alternative arrangements to obtain data from abroad through bilateral agreements such as the one being considered between the US and UK.

Part No.: II- SCOPE AND EXEMPTIONS

Chapter No.: 8- Cross-border Flow of Data

1. What are your views on cross-border transfer of data?

2. Should the data protection law have specific provisions facilitating cross border transfer of data? If yes, should the adequacy standard be the threshold test for transfer of data?

Yes, the data protection law must facilitate cross border sharing of data. However, Indian data protection laws in their current form are not among the most sophisticated in the world. Even under the new regime after the recommendations of the Srikrishna Committee have been accepted, the data protection rules will take years to mature and the rules thereunder to be particularised. In this backdrop, India should not adopt an adequacy standard for cross border transfer of Indian data. If India aims for a high threshold for determining adequacy, it is possible that very few countries will qualify; if on the other hand, India favors a lower threshold, then the adequacy requirements will be so diluted as to be redundant.

Instead, the new law should explore privacy impact assessments as a method of making data controllers accountable. Given that there are different stakeholders in the data chain such as the data controller, the data processor etc. the law should place differentiated responsibilities on each -- with the data controllers having the primary onus of the security and integrity of data.

4. Are there any other views which have not been considered?

India is a net exporter of data, which leads to value creation from Indian data outside Indian borders. The new data protection regime must recognise the need for prioritising the ability of Indian firms to build services based on Indian data. While this cannot take the form of protectionism, it can be operationalised through tie-in arrangements where Indian companies partner with foreign technology providers where services are provided on the basis of Indian data.

Part No.: IV- REGULATION AND ENFORCEMENT

Chapter No.: 2: Accountability and Enforcement Tools

D. Data Protection Authority

2. Is a separate, independent data protection authority required to ensure compliance with data protection laws in India?

3. Is there a possibility of conferring the function and power of enforcement of a data protection law on an existing body such as the Central Information Commission set up under the RTI Act?

4. What should be the composition of a data protection authority, especially given the fact that a data protection law may also extend to public authorities/government? What should be the qualifications of such members?

7. Considering that a single, centralised data protection authority may soon be overburdened by the sheer quantum of requests/ complaints it may receive, should additional state level data protection authorities be set up? What would their jurisdiction be? What should be the constitution of such state level authorities?

Yes, a separate independent data protection authority is required not just for compliance with data protection rules but also for raising awareness and specifying best practices. This responsibility cannot be delegated to any existing authorities, since their legislative mandate will need to be widened.

The new data protection authority (DPA) must have a clear legislative mandate and the Bill should lay out its constitution, powers and functions. This new body should ideally be a quasi- judicial body not unlike the National Company Law Tribunals that were constituted in 2016. Similar to the NCLT, the adjudicatory arm of the DPA must comprise of technical members from the central services such as the Indian Legal Service and the Indian Telecommunication Service. To address the challenge of of ensuring consistency in decision making, creation of expertise and increasing volume of cases, the law should prescribe the establishment of a one principal bench with the subsequent rollout of regional benches.

The adjudicatory arm of the DPA should be empowered to entertain class action lawsuits for two reasons: first, valuing quantum of loss is often difficult for individual cases of data breaches much less difficult when large data bases are compromised.. Second, this can also help reduce the number of cases before the authority where similarly affected cases can be heard and disposed off together.

In addition to the adjudicatory arm of the DPA, there must also be one arm that can conduct monitoring and investigation, and another dedicated to building capacity both internal and external. Similar to the director general of investigation under the Competition Commission of India, the investigative arm of the DPA should be empowered to conduct both suo moto investigation as well as on receiving complaints from users, after a prima facie finding by the adjudicatory arm. The capacity building arm should publish transparency reports and annual reports for effective monitoring.

Annexure I- List of Participants at ORF Data Protection Roundtables

1.	Amber Sinha	The Centre for Internet and Society
2.	Ambika Khurana	IBM
3.	Amitayu Sengupta	IAMAI
4.	Amitendra Singh Antal	Info Edge (India) Limited
5.	Anil Kumar Goel	Ministry of Social Justice & Empowerment
6.	Arjun Sinha	Consultant
7.	Arul Kumaran	Ministry of Electronics & Information Technology
8.	Arun Gandhi	TMI Group
9.	Arunima Sharma	Pepperfry
10.	Baijayant Panda	Member of Parliament
11.	Bedavyasa Mohanty	ORF
12.	Bhairav Acharya	Facebook
13.	Chetan Krishnaswamy	Google
14.	Chitrita Chatterjee	IAMAI
15.	Faiza Rahman	NIPFP
16.	Gargi Rohi	Vidhi Centre for Legal Policy
17.	Gaurav Gupta	National Informatics Centre
18.	Hardeep Singh	Uber
19.	K KMinocha	Formerly DOT
20.	Kamlesh Bajaj	Independent Consultant
21.	Kapil Chaudhary	Autodesk India Private Limited
22.	Kaushal Mahan	Chase India
23.	Khozem Merchant	Brunswick India
24.	Kriti Trehan	Law Offices of Panag&Babu
25.	Lalit Panda	Vidhi Centre for Legal Policy
26.	Madhulika Srikumar	ORF
27.	Mahesh Uppal	Com First (India) Private Limited
28.	Meghna Jalan	Office of Tathagata Satpathy
29.	Mishi Choudhary	Managing Partner, Mishi Choudhary & Associates
30.	Muni Shankar	Centre for Economic policy research
31.	Narendra K Gupta	ASEAN Chamber of Commerce
32.	Nayantara Menon Mehta	Uber

33.	Nayantara Narayan	Office of BJ Panda
34.	Nehaa Chaudhari	TRA | Lawyers for Innovation
35.	P.K.Jain	Min. of Power,C.E.A.
36.	Prachi Arya	Koan Advisory Group
37.	Pratibha Jain	Nishith Desai Associates
38.	Priyanka Chaudhuri	SFLC
39.	R Jai Krishna	TV18 Broadcast Ltd
40.	Radhika Rawat	Digital India Foundation
41.	Rahul Gupta	Delegation of the European Union to India
42.	Rahul Jain	Google
43.	Rajiv Chauhan	Ministry of Electronics & IT
44.	Rakhi Maheshwari	Amdar Consulting
45.	Robin Grewal	Sting Broadband
46.	Rohan Mitra	Adobe Systems India Pvt Ltd
47.	S. Prabhakhar	Parliament of India (Lok Sabha Secretariat)
48.	Samir Saran	ORF
49.	Samiran Gupta	ICANN
50.	Samraat Basu	Vidhi Centre for Legal Policy
51.	Sanya Dhillon	Office of BJ Panda
52.	SaritMaheshwari	NTPC limited
53.	Shagufta Kamran	USISPF
54.	Shivank Agarwal	Chase India
55.	Siddharth Singh	India Foundation (Foreign Policy Think Tank)
56.	Smriti Parsheera	NIPFP
57.	Sujeet Samaddar	NITI Aayog
58.	Ujjwal Bakshi	Chase India
59.	Ujjwal Kumar	CUTS International, Jaipur
60.	V K Tyagi	Ministry of Electronics & IT
61.	Varun Sen Bahl	PLR Chambers
62.	Venkatesh Krishnamoorthy	BSA
63.	Vidur Gupta	EY (Ernst & Young)