CUTS Submission to the Joint Committee on The Personal Data Protection Bill, 2019

CUTS International

D-217, Bhaskar Marg, Bani Park, Jaipur 302016, India
Tel: +91.141.2282821, Fax: +91.141.2282485
Email: cuts@cuts.org, Web site: www.cuts-international.org

Index

Background

In the judgement of K.S. Puttaswamy vs. Union of India, 2017,[1] the Supreme Court of India (SC) recognised 'right to privacy' as a fundamental right. The Government of India (GoI) had formed a committee to study various issues relating to data protection, which proposed the draft Personal Data Protection Bill 2018 (draft bill)[2]. After a round of public consultation, an amended Personal Data Protection Bill, 2019 (bill)[3] was introduced in Lok Sabha. The same has been referred to a Joint Committee of both houses of Parliament (JPC)[4] for review. Consumer Unity & Trust Society (CUTS)[5] expresses its gratitude to the JPC, for inviting comments and suggestions on it.

About CUTS

In its 35 years of existence, CUTS has come a long way from being a grassroots consumer-centric organisation based in Jaipur to opening overseas Resource Centres in Vietnam,[6] Africa,[7] Switzerland,[8] and most recently in the United States of America[9]. It continues to remain an independent, non-partisan and non-profit economic policy research and advocacy group, while working on various programme areas, such as Trade, Economics & Environment;[10] Consumer Action, Research & Training;[11] Human Development;[12] and Competition, Investment & Economic Regulation.[13] It has been working towards enhancing the regulatory environment through evidence-backed policy and governance-related interventions across various sectors and national boundaries. For further details regarding CUTS, please visit: http://cuts-international.org/pdf/About-CUTS-2018.pdf

---

1 Justice K S Puttaswamy (Retd.) and Another Vs. Union of India and Others; SC WP(C) No. 494 of 2012

2 Draft Personal Data Protection Bill 2018, available at: https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

3 The Personal Data Protection Bill 2019, available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

4 Members of the JPC, available at: http://loksabhaph.nic.in/Committee/CommitteeInformation.aspx?comm_code=73&tab=1

5 https://cuts-international.org/

6 http://cuts-hrc.org/en/

7 http://www.cuts-international.org/ARC/

8 http://www.cuts-geneva.org/

9 http://www.cuts-wdc.org/

10 http://www.cuts-citee.org/

11 http://www.cuts-international.org/CART/

12 http://www.cuts-international.org/CHD/

13 http://www.cuts-ccier.org/

Being a consumer-centric organisation, CUTS has observed a few critical issues in the bill, which impede consumer welfare, either directly or indirectly as a result of sub-optimal regulation and competition, in the market. A snapshot of the bill, entailing its highlights, lowlights, and proposed action points, has been given below. These are informed by CUTS' various evidence-based research initiatives:

- Consumer Impact Assessment of Data Localisation (CIA of DL)[14] wherein perspectives of 1300 users of digital technologies were considered to understand the impact of restrictions on cross border data flow on the usage of digital services.

- Data Privacy and User Welfare in India (Privacy Survey)[15] wherein perspectives of 2160 users of digital technologies with respect to data sharing, purposes thereof and risks therein were considered.

- Digital Trade and Data Localisation (DigiExpo)[16] wherein econometric modelling was utilised to determine the impact of restrictions on cross border data flow on digital exports.

[14] Objective: Assessing the impact of restriction of cross-border data flows on consumers, among other stakeholders, on parameters, such as quality of service, innovation, data privacy, data security etc. Expected Outcome: presenting an evidence-based impact of data localisation, to the government and other stakeholders. https://cuts-ccier.org/consumer-impact-assessment-on-cross-border-data-flow/

[15] Objective: Engage with consumers on a pan India level regarding data and privacy protection on both, online, as well as offline platforms, from the government and private players alike. Expected Outcome: Policy reforms empowering consumers for data privacy and protection. https://cuts-ccier.org/cdpp/

[16] Objective: Understand and analyse the importance of digital exports for India's GDP and economy, along with the possible impact of data localisation barriers on Indian exports of digital goods and services. Expected Outcome: build detailed and holistic understanding of the economic implications of existing and/or proposed data localisation barriers on India's digital exports, while producing evidence to study alternatives to data localisation measures which are prohibitory to free data flows, in order to help policy makers in India and around the world to take an informed and appropriates and on data localisation. https://cuts-ccier.org/pdf/project-brief-dtdl.pdf

The Bill at a Glance

The key highlights and lowlights of the bill have been given in the table below.

Highlights	Lowlights
• The bill grants various rights to data principals (users), such as data portability, correction and erasure of personal data, the right to be forgotten and grievance redress. • Differentiates between personal and sensitive personal data. • Mandates notice requirements, purpose limitation and transparency regarding processing personal data on data fiduciaries (service providers). • Bill provides for setting up a Data Protection Authority (DPA). • DPA has been empowered to create a 'sandbox' to encourage innovation. • A new concept of consent managers has been introduced.	• Implementation, awareness and capacity building issues remain unaddressed for the effective exercise of rights given to users. • Missed making significant data fiduciaries responsible for providing appropriate data protection tools to users. • Blanket exemptions are given to the GoI from the provisions of the bill, for processing personal data under various circumstances. • User perspective not considered while establishing 'identifiability' for the purpose of determining personal data. • Issues of consent and notice fatigue not addressed adequately. • GoI, in consultation with DPA, can direct service providers to provide anonymised and/or non-personal data for select purposes. • Details pertaining to 'sandbox' remain unknown and ambiguous. • The bill now provides for allowing users of social media intermediaries to voluntarily verify their accounts. • Data localisation, though minimised, but remains for sensitive and critical personal data.

Suggestions/action points for overcoming the lowlights have been tabulated below.

Action Points	
• Awareness and capacity building workshops for users must be undertaken, to enhance the uptake of data protection tools. • Cost-Benefit Analysis or impact assessment studies from a user and/or competition perspective must be undertaken on select provisions, to ensure optimal regulations. • Independence and accountability of DPA must be ensured. • Notices and privacy policies should be simple and easy to understand for users. Executive summaries may be prepared, and privacy labels should be adopted.	• Harsh provisions, such as data localisation should be removed, and less intrusive ways of ensuring Law Enforcement Agencies (LEAs) access to data need to be explored. • Explore alternate dispute redress mechanisms for users. • Greater accountability should be mandated on the GoI, and the exemptions must be pruned down while accommodating for compliance with the principles of the Puttaswamy judgement. • The regulatory overreach of the bill must be avoided, so as to not strive to attain government objectives that are beyond the scope of the bill. • JPC must hold extensive and inclusive stakeholders' consultations.

Recommended Clause by Clause Amendments in the Bill

Pursuant to the action points listed above, CUTS' recommends the following amendments in the bill.

A. Definitions (Details available in Annexure A)

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
3(28)	"personal data" means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling;	"personal data" means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any **physical, psychological, mental, cultural or social** characteristic, trait, attribute or any other feature of the identity of such natural person whether online, offline, or any combination of such features with any other information and shall include any inference drawn from such data for the purpose of profiling; **Explanation: For the purpose of determining identifiability, intimacy and necessity for such a**	Shortcomings: The possibility of 'identifying' natural person may differ with the relationship of such a natural person with the relevant data. Consequently, the absence of guidance to determine 'identifiability' may result in varying interpretations and vagueness. Recommendation: It might be useful to provide some identifiers and examples to elaborate on the concept of 'identifiability' to make it more specific. In this regard, it will also be important to consider user perception with respect to different kinds of data, i.e. the test for establishing 'identifiability' should include a user perception and perceived sense of users' intimacy and necessity of such data. This was validated through our Privacy Survey. Similar identifiers are also provided within the

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
		natural person of the data, including but not limited to name, number, address, location data, e-mail, will be considered.	European Union's (EU) General Data Protection Regulation (GDPR).[17]
3(36)	"sensitive personal data" means such personal data, which may reveal, be related to, or constitute— ……	"sensitive personal data" means such personal data, collection without consent, or **breach of which may result in physical, property, or psychological harm to data principals, including such personal data** which may reveal, be related to, or constitute…… **Passwords**	Shortcoming: No guiding principle is provided at present to distinguish sensitive personal data from personal data and justify greater protection to a subset of personal data. The definition also does not take into consideration, users' perception of privacy, associated risks and perceived sensitivity to certain kinds of data, such as passwords, which are users' first and only line of defence to protect their data. Recommendation: In order to distinguish sensitive personal data from personal data, the specification of associated harms caused due to the revelation of sensitive personal data may be useful. Such

[17] GDPR , Article 4(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
			specification is also prescribed under the Chinese Cyber Security Law.[18] In addition, passwords must be explicitly regarded as sensitive personal data.
33(2)	*Explanation*. — For the purposes of sub-section (*2*), the expression "critical personal data" means such personal data as may be notified by the Central Government to be the critical personal data.	*Explanation*. — For the purposes of subsection (*2*), the expression "critical personal data" means such **personal data, collection without consent, or breach of which can have a debilitating impact on national security, public health or safety** as notified by the Central Government to be the critical personal data.	Shortcoming: There is uncertainty in the definition of critical personal data, as there are no prescribed parameters for categorising such data. This results in wide discretion to the government for localising vast categories of data. Recommendation: Seeking inspiration from the Information Technology Act, which lays down the meaning of 'Critical Information Infrastructure'[19], similar parameters should be given for critical personal data.
3(20)	"harm" includes— …….....	"harm" **means the use of personal data, including personal data breach, resulting in**— ……....	Shortcoming: 'Harm' as prescribed in the bill lists certain outcomes which may be a result of the use of personal data or personal data breach and could adversely affect users. The definition in its current form does not make a clear linkage between

[18] Chinese Cyber Security Law, 2017

[19] Section 70 (1) "For the purposes of this section, —Critical Information Infrastructure‖ means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety."

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
			different harms and misuse of data. Recommendation: The provision must specify that harm must be linked to the use of personal data or personal data breach.

B. Notice and Consent (Details available in Annexure B)

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
7(2)	The notice referred to in sub-section (*1*) shall be clear, concise and easily comprehensible to a reasonable person and in multiple languages where necessary and practicable.	**Extension of this sub-section with the below line:** This will be in accordance with the model forms prescribed by the Authority under section 50(6)(a).	Shortcomings: The current provisions make a biased assumption of users being cognizant and capacitated of reading and understanding notices of data collection, as well as providing informed consent for the processing of their data. Notably, users today avail of numerous data-driven services, and notices from each service provider might burden users, and they may not be able/willing to spend time reading them (notice fatigue), thereby accepting them without any thought (consent fatigue). CUTS privacy survey highlighted that users do not read privacy policies (notices), mostly due to their length, which gets further encouraged
50(6)(a)	requirements for notice under section 7 including any model forms or guidance relating to notice;	(a) requirements for notice under Section 7 including any model forms or guidance relating to notice; **Explanation- for the purpose of sub-section (a), model forms shall mean privacy labels on the lines of nutrition labels or energy labels, which are a multi-**	

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
		lingual/info-graphic communication tool to provide clear, transparent and multi-layered privacy information to data principals. Sandbox provisions given under Section 40 may be used to test the efficacy of such privacy labels.	by the exhaustive list prescribed by S. 7(1). Few users who attempt to read them, do not understand them, due to excessive legalese or unfamiliar language. Recommendation: In order to maintain the efficacy of notice and consent, CUTS' proposes the bill to mandate the use of privacy labels, which can provide information in an easily understandable and accessible manner to users.
50(6)(d)	manner for obtaining valid consent under section 11;	a manner for obtaining valid consent under section 11**, including through model forms as mentioned in sub-section (a);**	

C. Exemptions (Details available in Annexure C)

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
35	Where the Central Government is satisfied that it is necessary or expedient, — (i) in the interest of sovereignty and integrity of India, the security of the State, friendly relations	**New section 35:** **(1) Processing of personal data by specified agencies of the Central Government without complying with specified provisions of this Act, shall not be permitted unless all the conditions**	Shortcomings: In the *Puttaswamy* Judgment-I,[20] it was held that privacy is not an absolute right, and could be overridden by the Central Government, subject to satisfying a three-prong legal test of legitimacy, proportionality, and

[20] Justice K S Puttaswamy (Retd.) and Another Vs. Union of India and Others SC WP(C) No. 494 of 2012

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
	with foreign States, public order; or (ii) for preventing incitement to the commission of any cognizable offence relating to sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, it may, by order, for reasons to be recorded in writing, direct that all or any of the provisions of this Act shall not apply to any agency of the Government in respect of processing of such personal data, as may be specified in the order subject to such procedure, safeguards and oversight mechanism to be followed by the agency, as may be prescribed.	**given below are met:** **a. it is in the interests of the security of the State.** **b. it is authorised pursuant to a law and is in accordance with the procedure established by such law, made by Parliament; and** **c. it is necessary for and proportionate to such interests and purpose of processing the data.** **Explanation – For the purposes of this section- (i) the term 'in the interests of security of the State' shall mean, - (a) in the interest of the sovereignty, security or integrity of India; and (b) for preventing the commission of any cognizable offence relating to the security of the state.** **(2) To process data in accordance with sub-section (1) above, the Central Government will make a written request**	legality. However, as opposed to the draft bill of 2018,[21] this test has been removed from Section 35 of the bill. Furthermore, exemptions based on a mere executive order is *ultra vires* of the *Puttaswamy* judgment II[22], wherein executive notifications were held to be insufficient for restricting the fundamental right to privacy. These issues fuel fears of surveillance by the government, and will therefore adversely affect free speech. Recommendation: CUTS' recommends incorporating the *Puttaswamy* test in the provisions of the bill by amending Section 35. Also, acquiring a judicial order for availing exemptions under the bill needs to be mandated.

21 Clause 42 of the Draft Bill of 2018

22 Justice K.S. Puttaswamy (Retd) vs Union of India, (2019) 1 SCC 1

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
		to a competent judicial authority, clearly stating: **a) reasons for invoking powers under sub-section (1) above.** **b) compliance with conditions mentioned in sub-section (1) above.** **c) Government agencies exercising powers and under sub-section (1) above and reasons thereof.** **d) Sections of the Act from which exemptions are sought, and reasons thereof.** **(3) The judicial authority will consider application made under sub-section (2) and make a reasoned order, which will be complied by the Central Government.**	
36	The provisions of Chapter II except section 4, Chapters III to V, Chapter VI except section 24, and Chapter VII shall not apply where— ……	**New section to be inserted after Section 36:** Personal data processed under Section 35, and sections 36(a), (b) and (c) shall not be retained once the purpose of security of the State; or investigation or prosecution of any	Shortcomings: The bill does not specify any limitation on the time for which personal data can be retained in case of collection for the exercise of exemptions. This could increase the chances of data being stored and used by government

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
		offence or other contravention of law; or enforcement of legal right; or judicial function; has been complete except where such personal data is necessary for the maintenance of any record or database which constitutes a proportionate measure to ensure security of the State; or investigate or prosecute any offence or class of offences; or enforce a legal right; or exercise judicial function, in future.	agencies or data fiduciaries beyond the purposes of the collection of data in such cases, putting the privacy of data principals at considerable risk.[23] Recommendation: The bill must place restrictions on retaining data for a period after the purpose of access to data has been achieved. Once, the purpose has been fulfilled, the same must be deleted by the data fiduciary.

D. Data Protection Authority (Details available in Annexure D)

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
42	(2) The Chairperson and the Members of the Authority shall be appointed by the Central Government on the recommendation made by a selection committee consisting of—	(2) The Chairperson and the Members of the Authority shall be appointed by the Central Government, **in compliance with the following process:** **(a) the Selection Committee will shortlist at least two candidates for each position through the procedure set out in sub-section 3, and nominate such candidates for hearing before the Parliamentary**	Shortcomings: The selection committee proposed by the bill for appointing members of the DPA only consists of executives of the Central Government, which diminishes the independence of the Authority while also fuelling risks of

[23] Justice B.N Srikrishna Committee Report, 2018

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
	(a) the Cabinet Secretary, who shall be Chairperson of the selection committee; (b) the Secretary to the Government of India in the Ministry or Department dealing with the Legal Affairs; and (c) the Secretary to the Government of India in the Ministry or Department dealing with the Electronics and Information Technology.	**Committee.** **(b) the Parliamentary Committee will conduct a hearing of candidates shortlisted by the Selection Committee, and nominate Chairperson and Members of the Authority.** **(c) The Central Government will appoint candidates nominated by the Parliamentary Committee as Chairperson and Members of the Authority.** **For the purpose of this section, the Selection Committee will consist of:** **(a) the Chief Justice of India or a judge of the Supreme Court of India nominated by the Chief Justice of India, who shall be the Chairperson of the selection committee;** **(b) the Cabinet Secretary;** **(c) an expert who has specialised knowledge of, and professional experience in the field of data protection, information technology, data management, data science, cyber and internet laws, and related subjects; nominated by the Chief Justice of India; and** **(d) Consumer rights expert or professional who has specialised knowledge of, and professional**	conflict of the result. Recommendations: In order to maintain the independence of the DPA, the selection committee should have a balance and include members from the judiciary, expert in data protection issues and consumer rights. This will protect the sovereignty of the regulator, and also ensure diverse and essential viewpoints from relevant stakeholders, for upholding privacy and data protection. In addition, in order to limit the role of government in appointment of members of the Data Protection Authority, it will be important that the final selection of candidates is conducted by a Parliamentary Committee through hearing.

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
		experience in the field of consumer rights, associated with data protection, digital economy, and related areas; nominated by the Department of Consumer Affairs. **Explanation: For the purpose of this section, the Parliamentary Committee will mean the Parliamentary Standing Committee on Information Technology.**	
42(3)	The procedure to be followed by the Selection Committee for recommending the names under sub-section (*2*) shall be such as may be prescribed.	**Procedure to be followed by the Selection Committee** **(a) The Selection Committee must make a document stating the procedure it will follow for selecting from candidates.** **(b) The procedure must be fair, transparent and efficient.** **(c) The Selection Committee must advertise the vacancy and the procedure for selecting candidates to attract the attention of suitable candidates.** **(d) The Selection Committee may consider candidates who have not applied after recording reasons for considering such candidates. Persons working as**	Shortcoming: The bill does not prescribe any basic minimum transparency requirements for the selection process. Recommendation: Procedure to be followed by a selection committee has been elaborately laid out under the draft Indian Financial Code.[24] Inspiration may be taken from the same for provisions of this bill as well.

[24] https://www.prsindia.org/uploads/media/draft/Draft-%20Indian%20Financial%20Code,%202015.pdf

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
		members or chairpersons in other regulatory agencies or authorities, may also be invited to apply. **(e) The Selection Committee must complete its selection procedure within ninety days of being constituted.**	
49(1)	The Authority may appoint such officers, other employees, consultants and experts as it may consider necessary for effectively discharging of its functions under this Act.	**New sub-section to be inserted as 49(1)(a):** The Authority shall through a written order, and after following due process as stipulated by regulations, designate experienced and credible consumer organisations as authorised consumer assistance centres, which will act as mediators between data principals and data fiduciaries, for resolving any grievances of data principals. Explanation: for the purpose of sub-section (1)(a), an authorised consumer assistance centre shall: perform one or more of the following functions - counselling, drafting complaints and providing information; and can extend one or more of the following services - grievance redress, mediation, legal assistance, class action, claiming compensation, enabling consumer participation in sandbox, reviewing safeguards offered in sandbox, awareness generation, capacity building, and training.	Shortcoming: In order to make data protection reality for consumers, credible consumer organisations will need to be co-opted for the cause. The bill does not provide for the same at present. Recommendation: As has been discussed subsequently in our submission, CUTS' recommends setting up consumer assistance centres, tasked with raising awareness, building capacity and facilitating grievance redress for users. Such centres can also help users participate in a sandbox, file complaints and claim compensations under

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
			the bill.
66(2)	All sums realised by way of penalties under this Act shall be credited to the Consolidated Fund of India.	All sums realised by way of penalties under this Act shall be credited to the **Data Protection Awareness Fund**.	Shortcoming: CUTS privacy survey highlighted users' low levels of understanding of issues of data protection and privacy. Recommendation: On the lines of consumer welfare fund set up under the Central Excise and Salt Act,[25] the CGST Act 2015,[26] the Telecommunication Consumers Education and Protection Fund,[27] the bill must retain such funds for purposes mentioned under the draft bill of 2018, and beyond.
79	(2) The Data Protection Authority Fund shall be applied for meeting— (i) the salaries, allowances and other remuneration of the Chairperson, Members, officers, employees, consultants and experts appointed by the Authority; and (ii) the other expenses of the Authority in connection with the discharge of its functions	(2) The Data Protection Authority Fund shall be applied for meeting— -- **(3) Without prejudice to the foregoing, there shall also be constituted a fund to be called the Data Protection Awareness Fund to which all sums realised by way of penalties by the Authority under this Act shall be credited.** **(4) The Data Protection Awareness Fund shall be applied solely for the purpose of generating awareness regarding data protection for the rights of data principals as mentioned under Chapter V and for other purposes as may be required and considered**	

25 Innovative Funding for Consumer Groups, Intergovernmental Group of Experts on Consumer Law and Policy, 2017

26 https://consumeraffairs.nic.in/organisation-and-units/division/consumer-welfare-fund/overview

27 www.trai.gov.in/sites/default/files/201209030250489400257regulation15jun07%5B1%5D.pdf

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
	and for the purposes of this Act	**appropriate for the welfare of data principals.** **(5) The Data Protection Authority may provide funding, and collaborate with experienced and credible consumer rights organisations, to comply with the objective in sub-section (4).**	
15(1)	The Central Government shall, in consultation with the Authority and the sectoral regulator concerned, notify such categories of personal data as "sensitive personal data", ……	The **Data Protection Authority, in consultation with the sectoral regulator concerned**, notify such categories of personal data as "sensitive personal data", …….	Shortcoming: the power of DPA (as granted by the previous draft bill) to notify categories of sensitive personal data has been shifted to the central government. Such dilution of powers of the DPA in favour of the central government is not advisable since the DPA as a regulator would be better equipped with the knowledge, experience, and information pertaining to data practices, as compared to the central government. Recommendation: CUTS recommends the shifting of this power back to the DPA. Decision

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
			making by the central government, despite having an expert dedicated regulator would potentially delay decision making, while also fuelling risks of political biases and conflict of interests.
94(2)	In particular and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely: — ……	**New sub-section to be inserted as 94(2)(t):** the procedure of designating experienced and credible consumer organisations as authorised consumer assistance centres under section 49(1).	Discussed in the section of grievance redress.
94	(*1*) The Authority may, by notification, make regulations consistent with this Act and the rules made thereunder to carry out the provisions of this Act. (*2*) In particular and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters,	**New sub-section to be inserted as 94(3):** 1) The Authority must publish a draft of a proposed regulation, accompanied with a statement setting out, – (a) the objectives of the proposed regulation; (b) the problem that the proposed regulation seeks to address; (c) how solving this problem is consistent with the objectives of the Authority under this Act;	Shortcoming: Despite having wide powers under this sub-section, the DPA has not been mandated to ensure adequate transparency while issuing regulations. There is no requirement to undertake cost-benefit analysis (CBA), public consultation while framing regulations or periodically

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
	namely: — …….	(d) the manner in which the proposed regulation will address this problem; (e) the manner in which the proposed regulation complies with the provision of this Act under which the regulation is made; (f) an analysis of costs and an analysis of benefits of the proposed regulation; (g) the process by which any person may make a representation in relation to the proposed regulation For the purpose of this sub-section, when carrying out an analysis of costs and benefits, the Authority must consider probable costs that will be borne by and the probable benefits that will accrue to persons affected by the regulation, including, the data fiduciaries, data principals, and the Authority. The Authority must use the best available data, and wherever not available, reasonable estimates, to carry out the analysis; and the most appropriate scientific method available to carry out the analysis. 2) The Authority must: a) give a time of not less than thirty days to enable any	reviewing them. Recommendation: The bill must mandate adopting scientific regulatory decision-making processes, in order to frame optimal regulations, wherein the costs of regulations do not outweigh its intended benefits. The Authority must undertake time-bound public consultation and should also review the justification of regulations from time to time. Inclusion of sunset clauses for regulations have been recommended in this regard. Inspiration may be taken from the Indian Financial Code in this regard.

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
		person to make a representation in relation to the proposed regulation and consider all representations made to it within that time. b) publish all the representations received by it along with a general account of the response of the Authority to the representations. 3) If the regulations differ substantially from the proposed regulations, the Authority must publish the details and reasons for such difference; and an analysis of costs and an analysis of benefits, of the differing provisions. 4) (1) The Authority must review every regulation made by it within three years from the date on which that regulation is notified. The review must comprise an analysis of: a) costs and an analysis of benefits of the regulation; b) all interpretations of the regulation made by relevant quasi-judicial and judicial authorities; and (c) the applicability of the regulation to any change in	

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
		circumstances since that regulation was issued. (2) The report prepared by the Authority of such review should be made public. (3) Unless notified again before the conclusion of three years of notification of regulation and three months within its review, a regulation will automatically lapse and cease to remain in force from the completion of three years of its notification.	

E. Grievance Redress (Details available in Annexure E)

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
32(2)	A data principal may make a complaint of contravention of any of the provisions of this Act or the rules or regulations made thereunder, which has caused or is likely to cause harm to such data principal,	A data principal may make a complaint of contravention of any of the provisions of this Act or the rules or regulations made **thereunder, to**…… **(c) an authorised consumer assistance centre, as authorised by**	Shortcomings: As discussed previously, CUTS' privacy survey had pointed out, that only a few users who experienced a personal data breach or a privacy violation, went on to complain about it. Users were also found to be unaware regarding the avenues of registering their grievances. Recommendations: As discussed previously, the DPA

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
	to— (*a*) the data protection officer, in case of a significant data fiduciary; or (*b*) an officer designated for this purpose, in case of any other data fiduciary.	**the Authority under section 49(1)(a).**	may introduce mediation mechanisms on the lines of CUTS *Grahak Sahayta Kendra*.[28] In addition, the complaint must not be contingent upon the harm caused to the data principal. In other words, mere contravention of provisions of the Act should be sufficient for data principals to file a complaint, whether or not resulting in associated harm.
32(4)	Where a complaint is not resolved within the period specified under sub-section (*3*), or where the data principal is not satisfied with the manner in which the complaint is resolved, or the data fiduciary has rejected the complaint, the data principal may file a complaint to the Authority in such manner as may be prescribed.	**New sub-sections to be inserted as 32(5) and (6):** (5) A complaint made under sub-section (*4*) shall be resolved by the Authority in an expeditious manner and not later than sixty days from the date of receipt of the complaint by the Authority. (6) Any order passed for resolving a complaint referred to in sub-section (5) shall specify the reasons in writing for providing or not providing relief to the data principal.	Shortcomings: No time limit has been prescribed by the bill at the level of the DPA as well as the Appellate Tribunal to dispose of any complaints made by users, which may deter them from pursuing their complaints in case of delays in getting their grievances redressed. Also, no provision has been made by the bill, for the DPA to provide a reasoned order with respect to complaints filed by users. Recommendations: Informed by the Consumer Protection Act 2019, a timeline for not more than sixty days may be provided for resolutions of complaints at the level of the DPA.

[28] https://cuts-cart.org/consumer-care-centre-grahak-sahayta-kendra/

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
		(7) In case if the relief is not provided under sub-section (5), the Authority shall inform the data principal regarding the right to file a complaint with the Appellate Tribunal against the order, within such period and in such manner as may be specified by regulations.	
64(1)	Any data principal who has suffered harm as a result of any violation of any provision under this Act or the rules or regulations made thereunder, by a data fiduciary or a data processor, shall have the right to seek compensation from the data fiduciary or the data processor, as the case may be.	**Any data principal shall have the right to seek compensation from the data fiduciary or the data processor, as the case may be, on account of any violation of any provision under this Act or the rules or regulations made thereunder, by such data fiduciary or data processor.**	Shortcoming: The provision in its current form, only gives users' right to claim compensation if they have suffered harm. Assessment of and establishing the harm suffered, limits their right to compensation. Recommendation: Users' right to claim compensation should not be contingent on harm. Rather violation of any provision of the bill itself should be ground enough to claim compensation.
83(2)	No court shall take cognizance of any offence under this Act, save on a complaint made by the Authority	**A court shall take cognizance of any offence under this Act, on:** **a) a complaint made by the Authority; or**	The court should be given the power to take cognizance of the complaints made by the data principals which in the current bill is only limited to the complaints made by the DPA. Similar limited provision was struck down by the Supreme Court

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
		b) a complaint made by the data principal.	under the *Puttaswamy* Judgement,[29] hence necessary changes must be made within the current bill. A similar practice is followed in the EU's GDPR, which gives the right to data subject to access appropriate judicial remedy.[30] In order to provide for an alternate recourse, consumer assistance centres might be set up on the lines of CUTS *Grahak Sahayta Kendra*,[31] which are specifically focused on consultation and conciliation on consumer complaints.
25(1)	Every data fiduciary shall by notice inform the Authority about the breach of any personal data processed by the data fiduciary where such breach is likely to cause harm to any data principal.	Every data fiduciary shall by notice inform the Authority about the breach of any personal data processed by the data fiduciary**. It shall also disclose details of such breach in the public domain, including its website.** **New sub-section to be inserted as 25(1)(a):**	Shortcomings: The bill currently, only provides for notification of the breach to users after the assessment by the DPA regarding the severity of harm, which delays information pertaining to risks emanating from such data breach, being relayed to users. Also, sole discretion of determining possible harm to users may not be given to service providers, and

29 Justice K S Puttaswamy (Retd.) and Another Vs. Union of India and Others; SC WP(C) No. 494 of 2012

30 GDPR, Article 78 "Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them."

31 "Consumer Care Centre (Grahak Sahayta Kendra) | CUTS Centre for Consumer Action Research & Training (CART)," https://cuts-cart.org/consumer-care-centre-grahak-sahayta-kendra/.

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
		When the personal data breach is likely to result in harm to data principals, the data fiduciary shall communicate the personal data breach to the data principal without undue delay, through personal means like emails, notifications and messages, along with specific actions required to be taken by them to mitigate the likely harm caused by such breach. Notwithstanding anything contained in this clause, the data principal will not be liable for failure to take actions mitigating likely harm.	every data breach at their end may be reported to the Authority. Recommendation: CUTS, therefore, recommends service providers affected by a data breach to inform their users of such breach without undue delay. This practice is also followed in the EU's GDPR[32] and China's Cyber Security Law. In case of likelihood of harm, personalised means could be used to inform about the breach, while in other cases, disclosure in public domain could suffice. Also, in order to raise the accountability of service providers, they should be mandated to disclose all breaches of personal data to the Authority, irrespective of the likelihood of harm to be caused to users.

[32] GDPR, Article 34 "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."

F. Cross-Border Data Flows (Details available in Annexure F)

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
33(1)	(1) Subject to the conditions in sub-section (1) of section 34, the sensitive personal data may be transferred outside India, but such sensitive personal data shall continue to be stored in India.	**This sub-section may be removed and a new sub-section may be inserted as 91(2):** Nothing in this Act shall prevent the Central Government from entering into a bi-lateral or multi-lateral agreement with other countries, or with any data fiduciary, domestic or foreign, for purposes mentioned in sections 35 and 36, subject to the provisions mentioned therein.	Shortcomings: CUTS study 'CIA of DL' has highlighted the adverse impact of DL on users in terms of possible reduced uptake of select data-driven services, such as e-commerce, social media and communication services. It also suggests that DL is expected to enhance risks of privacy violation, cyber-attacks and data breaches, while adversely impacting the availability of services and curbing innovation. Another CUTS study 'DigiExpo' showcased the adverse impact of DL on India's IT-BPM industry, with respect to digital services export. The scope and extent of data restrictiveness may plunge the digital services exports between 10 to 19 percent, which may in turn adversely affect the gross domestic product (GDP) by 0.18 to 0.35 percent. Recommendations: Instead of imposing DL, the government should focus on exploring less intrusive means of achieving its legitimate regulatory objectives. It may enter into multilateral and bilateral agreements for ensuring valid LEAs access to data. With respect to economic development, encouraging domestic innovation and creating jobs, a separate

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
			policy to incentivise processing of data in India may be formulated, instead of forcing DL (as has also been called for in budget 2020)[33].

G. Overreach of the Bill (Details available in Annexure G)

Clause	Provisions to be Removed from the Bill	Reasons / Remarks
26(4)	Notifying social media intermediaries as significant data fiduciaries.	User verification intuitively seeks to solve the problem of inappropriate posts/information through this legislation, which may be considered an overreach, since it does not fall within the ambit of personal data protection, and is already being deliberated upon in The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018.[34] CUTS in its submission of comments on the same flagged how the provisions of the amendment rules are antithetical to privacy and anonymity, and also highlighted the various compliance costs it may impose on service providers.[35]
28 (3) and (4), 93(2)(d)	Voluntary user verification	
91(2)	Government's access to anonymised personal data and non-personal data.	The bill empowers the GoI to get access to non-personal data, or anonymised personal data processed by service providers (data fiduciaries), for select regulatory objectives. However, such a provision appears to be beyond the scope of the bill. The

33 https://www.livemint.com/news/india/govt-s-nudge-may-help-india-become-a-global-data-centre-11580664564132.html

34 https://meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf

35 https://cuts-ccier.org/pdf/CUTS_comments_on_the_Information_Technology_Intermediary_Guidelines.pdf

Clause	Provisions to be Removed from the Bill	Reasons / Remarks
2(B)	shall not apply to the processing of anonymised data, **other than the anonymised data referred to in section 91**.	provision also runs the risk of overlap with a separate committee chaired by Kris Gopalakrishnan, which is deliberating on framing governance norms for non-personal data.[36] Also, forced access to such data may infringe on the intellectual property rights of service providers pertaining to such data.

H. Transitional Provisions

Provisions to be Added in the Bill	Reasons / Remarks
Chapter XIV on 'Transitional Provisions', i.e. S. 97 of the Draft Personal Data Protection Bill 2018, should be appropriately retained in the Bill.	The bill does not prescribe any time limit to set up the DPA. This coupled with the absence of transitional provisions as given in the draft bill, may lead to uncertainty for service providers. It may become difficult to interpret if all the provisions of the bill will come into force with immediate effect upon enactment, or in a phased manner. Furthermore, users also run the risk of their rights towards their personal data being guaranteed by law, but without any effective machinery to enforce them, or seek remedy against any grievances.[37]

I. Other Recommended Amendments

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks

[36] https://www.medianama.com/2019/09/223-meity-non-personal-data-committee/

[37] https://www.dvara.com/research/wp-content/uploads/2020/01/Initial-Comments-on-the-Personal-Data-Protection-Bill-2019.pdf

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
Purpose Limitation			
5	Every person processing personal data of a data principal shall process such personal data— (b) for the purpose consented to by the data principal or which is incidental to or connected with such purpose, and which the data principal would reasonably expect that such personal data shall be used for, having regard to the purpose, and in the context and circumstances in which the personal data was collected.	Every person processing personal data of a data principal shall process such personal data— (b) for the purpose consented to by the data principal or **which is compatible with such purpose**, and which the data principal would reasonably expect that such personal data shall be used for, having regard to the purpose, and in the context and circumstances in which the personal data was collected.	Shortcoming: CUTS privacy survey exposed the awareness gap, and capacity constraints of users, on issues related to privacy and data protection. Accordingly, mechanisms such as purpose limitation become extremely relevant for avoiding excessive processing of data by service providers. Recommendation: The bill may mandate any processing of personal data to be compatible with the original purpose of processing. This will promote innovation without enhancing privacy risks. This is also on the lines of the Asia Pacific Economic Cooperation (APEC) Privacy Framework.
Offences			

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
82(1)	Any person who, knowingly or intentionally— (*a*) re-identifies personal data which has been de-identified by a data fiduciary or a data processor, as the case may be; or (*b*) re-identifies and processes such personal data as mentioned in clause (*a*), without the consent of such data fiduciary or data processor, then, such person shall be punishable with imprisonment for a term not exceeding three years or with a fine which may extend to two lakh rupees or both.	Any person **who alone or jointly with others,** knowingly or intentionally **or recklessly—** ….. **(c) obtains personal data; or** **(d) discloses personal data; or** **(e) transfers personal data to another person; or** **(f) sells or offers to sell personal data to another person,** without the consent of such data fiduciary or data processor, then, such person **or persons** shall be punishable with imprisonment for a term not exceeding three years or with a fine which may extend to two lakh rupees or both. **New sub-section to be inserted as 82(2):** In case, the personal data mentioned in sub-section (1) is sensitive personal data, then such person or persons shall be punishable with imprisonment for a term not exceeding five years or shall be liable to a fine which may extend up to rupees three lakhs or both.	Shortcoming: CUTS privacy survey pointed out that users are concerned about the unauthorised transfer of their personal data to third parties. However, the bill has removed the offence for obtaining, transferring and selling of personal data, which might limit the users' rights. Recommendation: In order to ensure adequate data protection for users, offences for non-consensual acquisition, disclosure, transfer or sale of personal data must be made punishable, as was the case in the draft bill of 2018.
Co-ordination between Authority and other regulators or authorities			

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
56	Where any action proposed to be taken by the Authority under this Act is such that any other regulator or authority constituted under a law made by Parliament or the State legislature may also have concurrent jurisdiction, the Authority shall consult such other regulator or authority before taking such action and may also enter into a memorandum of understanding with such other regulator or authority governing the coordination of such actions	Where any action proposed to be taken by the Authority under this Act is such that any other regulator or authority constituted under a law made by Parliament or the State legislature may also have concurrent jurisdiction, the Authority shall consult such other regulator or authority before taking such action **by:** **(i) entering into a memorandum of understanding with such other regulators or authority governing the coordination of such actions; or** **(ii) making a reference in respect of such action to such other regulator or authority.** **On receipt of a reference under this sub-section, the other regulator or authority shall give its opinion, within sixty days of receipt of such reference, to the Authority which shall consider such opinion, and thereafter take such action, after recording the reasons thereof.**	Many of the data protection provisions within the bill overlap with policies conceptualised or implemented in sectors such as ePharmacies, Fintech sector, eCommerce, Telecom sector, etc. For better coordination, provisions of the Competition Act 2002 may be adapted in the bill, which provides for coordination with the Competition Commission of India (the market regulator) with sector-specific regulators.
Sandbox for encouraging innovation			
40(4)	(b) the safeguards including terms and conditions in view of the obligations under clause (c) including the requirement of	(b) the safeguards including terms and conditions in view of the obligations under clause (c) including the requirement of consent of data principals participating under any licenced activity, **notifying data principals**	The bill has largely been silent on user protection in the sandbox. Making matters worse are the exemptions given in

Clause	Original Provision in the Bill	Proposed Amended Provision	Reasons / Remarks
	consent of data principals participating under any licensed activity, compensation to such data principals and penalties in relation to such safeguards. (c) that the following obligations shall not apply or apply with a modified form to such data fiduciary, namely: —	**of potential risk,** compensation to such data principals and penalties in relation to such safeguards. (c) **the sub-section should be removed.**	40(4)(c), which must be removed.

The Way Forward

CUTS' looks forward to the JPC accepting the proposed amendments given above, and to assist the JPC in its endeavours of securing citizens' personal data. **We are also keen to present our evidence-based recommendations to the JPC and would request for a suitable date and time for an in-person representation before the JPC .**

Also, considering the elaborate changes made from the previous draft bill, coupled with the suggestions given above, we urge the JPC to kindly hold extensive and inclusive open house discussions on the bill, before finalising its report.

For any clarifications/further details, please feel free to contact Amol Kulkarni (amk@cuts.org), Sidharth Narayan (sid@cuts.org) and/or Shubhangi Heda (sbg@cuts.org).

Annexure – A: Key Definitions in the Personal Data Protection Bill 2019

Introduction

The Personal Data Protection Bill 2019 (bill),[38] warrants its functioning and implementation on key operational definitions. In this regard, various terms such as: 'personal data',[39] 'sensitive personal data',[40] 'critical personal data',[41] 'harm'[42] etc. have been defined under the bill. Some of these definitions suffer from ambiguities, and can result in broad and varying interpretations.

Clarity in the scope of these terms is pertinent to understand the expanse of the bill, with respect to rights of data principals (users), obligations of data fiduciaries (service providers), restrictions on cross-border data flows, offences, penalties and claims for compensation. Hence, evaluation of these terms in specific contexts becomes essential to assess the application of bill and its effect on various stakeholders.

Assessment of Definitions

Personal Data -

"personal data" means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling.

In its current form, the definition of personal data is contingent upon 'identifiability' of the person through such data. But, this criterion of 'identifiability' may differ depending upon the social, economic, cultural profile and intimacy of the person towards relevant data. This is also informed by the CUTS user perception survey on privacy and data protection, which observed that different users (based on gender, age, years of using internet etc.) perceive different information differently. For instance, female users are more uncomfortable in sharing their email-ids, compared to male counterparts or more adults are uncomfortable in sharing their personal photos compared to younger people.[43] Hence, it is important to consider user perspectives while determining 'identifiability'.

38 The Personal Data Protection Bill 2019. Available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

39 S. 3(28) of the Bill

40 S. 3(36) of the Bill

41 S 33 of the Bill

42 S. 3(20) of the Bill

43 Amol Kulkarni and Swati Punia, "Users' Perspectives on Privacy and Data Protection" (Jaipur: C-CIER, CUTS International).

Also, the possibility of 'identifying' natural person may differ with relationship of such natural person with the relevant data. Consequently, absence of guidance to determine 'identifiability' may result in varying interpretations and vagueness.

It might be useful to provide some identifiers and examples to elaborate on concept of 'identifiability' to make it more specific. In this regard, it will also be important to consider user perception with respect to different kinds of data, i.e. the test for establishing 'identifiability' should include a user perception and perceived sense of intimacy and necessity of such data. This was validated through our Privacy Survey. Similar identifiers are also provided within European Union's (EU) General Data Protection Regulation (GDPR).[44]

Sensitive personal data -

"sensitive personal data" means such personal data, which may, reveal, be related to, or constitute— (i) financial data; (ii) health data; (iii) official identifier; (iv) sex life; (v) sexual orientation; (vi) biometric data; (vii) genetic data; (viii) transgender status; (ix) intersex status; (x) caste or tribe; (xi) religious or political belief or affiliation; or (xii) any other data categorised as sensitive personal data under section 15.

The definition of 'sensitive personal data' specifies types of data such as financial data, health data, official identifier etc. The aim of categorisation of 'personal data' and 'sensitive personal data' separately is to provide more protection to certain types of data which are sensitive to the users. Although, this premise doesn't come out of the definition in a clear way, as it must also reflect users' perceived risk of misuse along with providing a guiding principle for categorisation of such data.

In this regard, being informed by the Chinese Cyber Security Law[45] and Japan's Act of the Protection of Personal Information (APPI),[46] a guiding principle of associated harm with revelation of data may be provided in the definition of 'sensitive personal data'. It can specify that the definition includes such data which if revealed can cause 'psychological, property or physical harm'.[47] Such specification will help categorisation of data through risks of such harm, justifying its sensitivity for the users.

Further, the definition excludes passwords from sensitive personal data. As observed in CUTS', survey, users don't use data protection tools making passwords their first and only line of defence for data protection.[48] Hence, **passwords should be reinstated within the definition of 'sensitive personal data'.**

44 GDPR , Article 4(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

45 Chinese Cyber Security Law 2017

46 Japan's Act of the Protection of Personal Information (APPI), https://www.ppc.go.jp/en/

47 Chinese Cyber Security Law 2017

48 Amol Kulkarni and Swati Punia, "Users' Perspectives on Privacy and Data Protection" (Jaipur: C-CIER, CUTS International).

Critical personal data -

"critical personal data" means such personal data as may be notified by the Central Government to be the critical personal data.

There is uncertainty in this definition, as there are no prescribed parameters for categorising such data. This results in wide discretion to the government for localising vast categories of data. **Seeking inspiration from the Information Technology Act, which lays down the meaning of 'Critical Information Infrastructure'[49], the definition may lay down specific parameters such as: *unauthorised collection, or breach of personal data which can have debilitating impact on national security, public health or safety should be given for critical personal data*.**

'Harm' -

"harm" includes— (i) bodily or mental injury; (ii) loss, distortion or theft of identity; (iii) financial loss or loss of property; (iv) loss of reputation or humiliation; (v) loss of employment; (vi) any discriminatory treatment; (vii) any subjection to blackmail or extortion; (viii) any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal; (ix) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; or (x) any observation or surveillance that is not reasonably expected by the data principal;

'Harm' as prescribed in the bill lists certain outcomes which may cause adverse effect for users, but does not make a clear linkage to misuse of data. Further, the scope of the definition is limited as it does not take into account new risks which might have to be addressed with evolution of technology.[50] This creates ambiguity and confusion for users and service providers, and limits the rights of users to only listed harms. **To address this, the bill must provide a broader definition of harm, also appropriate guidelines regarding its interpretation to establish linkages with harms as listed to the personal data breach must be laid down. This could be through specifying that such harm must be caused through processing of personal data or caused through personal data breach in contravention to the bill.**

49 Section 70 (1) "For the purposes of this section, —Critical Information Infrastructure‖ means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety."

50 Srikara Prasad, "An Analysis of 'Harm' Defined under the Draft Personal Data Protection Bill, 2018," *Dvara Research Blog* (blog), 2019, https://www.dvara.com/blog/2019/10/29/an-analysis-of-harm-defined-under-the-draft-personal-data-protection-bill-2018/.

Annexure – B: Notice and Consent Framework of the PDPB *The Way Forward*

Background

The Personal Data Protection Bill (PDPB) 2019[51] under S. 7(1) mandates service providers (data fiduciaries) to give notice to users (data principals) regarding the collection of their personal data with respect to the purpose and terms of data processing, rights available to users, among other details. Furthermore, S. 7(2) prescribes that notice to be clear, concise and easily comprehensible to a reasonable person.

With respect to consent, S. 11(1) necessitates service providers seek the consent of users before processing their personal data. The next sub-section, i.e. 11(2), lays down the principles of valid consent that it should be free, informed, specific, clear and capable of being withdrawn. The concept of consent managers has been introduced under S. 23 of the PDPB, which are required to be registered with the Data Protection Authority (DPA), and seek to provide a centralised consent management mechanism to users.

Shortcomings of these Provisions

Though the above provisions intend to provide useful protection to users against the processing of their data without their consent, doubts remain on the efficacy of the provisions, due to the nuances of notice and consent frameworks.

Lack of awareness of privacy policies: The provisions make a biased assumption of users being cognizant and capacitated of reading and understanding notices of data collection, as well as providing informed consent for the processing of their data. CUTS' user perception survey[52] on privacy and data protection pointed out that most people don't read privacy policies (notices), mostly due to their exhaustive length. Few users who attempt to read them, do not understand them, due to excessive legalese.

Service providers should not be allowed to use notices as a means to shrug away from

51 PDPB 2019, accessible at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

52 Kulkarni, Amol and Swati Punia, "Users' Perspectives on Privacy and Data Protection" (C-CIER, CUTS International, n.d.). Available at: https://cuts-ccier.org/cdpp/

their liability of data collection disclosure. On the contrary, the essence behind them should be to inform users about service providers' data processing practices and enable them to compare policies while making their decision. In this regard, PDPB has omitted the requirement for providing the 'Data Protection Awareness Fund' for capacity building and awareness generation activities which were stipulated in the Draft Bill of 2018.

Notice and consent fatigue: Users today avail of numerous data-driven services. Notices from each of the many service providers might burden users, and they may not be able/willing to spend time reading them (notice fatigue), thereby accepting them without thought.[53] A similar observation was also made in a recent study,[54] which concluded that after the implementation of European Union's (EU) General Data Protection Regulation (GDPR), there has been an increase in consent notices to be accepted by users, which has led to them being fatigued with such notifications. Hence, the bill should include provisions for encouraging innovation in privacy-enhancing technologies pertaining to notice and consent mechanisms that are accessible and consumer-friendly.

Consent Managers: In order to address the issue of consent fatigue, the bill introduces the use of consent managers. This is somewhat similar to the Account Aggregator (AA) mechanism which provides a centralised framework for providing consensual sharing of information with financial service providers through Data Protection and Empowerment Architecture (DEPA). Such mechanisms are new for users and there are concerns regarding the acceptability of such infrastructure and familiarity of its functioning by users and there adherence to privacy by design policies as proposed in PDPB.[55]

Also, various questions remain to be answered such as: how will interoperability of consent managers be functional as there exists a large number of service providers; are consent managers going to be sector-specific, or generic; and how and will the DPA regulate all consent managers etc. Furthermore, there is a need to weigh the security risks posed by having a centralised consent dashboard.

53 Rishab Bailey et al., "Disclosures in Privacy Policies: Does' Notice and Consent' Work?" (New Delhi: NIPFP, 2018).

54 Christine Utz et al., "(Un)Informed Consent: Studying GDPR Consent Notices in the Field," *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, November 6, 2019, 973–90, https://doi.org/10.1145/3319535.3354212.

55 Raghavan and Singh, "Building Safe Consumer Data Infrastructure in India: Account Aggregators in the Financial Sector (Part–2)," *Dvara Research Blog* (blog), accessed on February 04, 2020, https://www.dvara.com/blog/2020/01/07/building-safe-consumer-data-infrastructure-in-india-account-aggregators-in-the-financial-sector-part-2/.

Recommendations

Data Protection Awareness Fund: PDPB should provide for the creation of a 'Data Protection Awareness Fund,'[56] which could specifically be used for increasing users' knowledge regarding the mechanisms through which they can better exercise their rights under PDPB. This would also assist in making users more acceptable and familiar to consent managers. For this, there should be a provision for funding experienced and credible civil society organisations to undertake user awareness generation and capacity building activities.

Innovation for User-Friendly Consent and Notice Mechanisms: The sandbox[57] should be used to promote innovation for consumer-friendly consent mechanisms, like consent manager/dashboards. This will improve research and experimentation to come up with consumer-friendly designs specifically suiting Indian demographics.

Transitional Provision and Codes of Practice: The codes of practice[58] may specifically require the DPA, to hold adequate and inclusive stakeholder consultation for coming up with guidelines for innovation of technology for easily accessible and understandable notices for users, like privacy labels. Regulatory Impact Assessment (RIA) may also be conducted in this regard, in order to ensure that the costs of regulations, do not outweigh its intended benefits. Also, transitional provision must be introduced for introducing guidelines for consent managers to remove the uncertainty and provide for more predictability for businesses.

56 The same provided under S. 77(2) of the draft Personal Data Protection Bill, as prepared by the BN Srikrishna Committee. Available at: https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

57 As provided under S. 40 of the bill.

58 As provided under S. 94(2)(h)

Annexure – C: Exemptions for the State

The Personal Data Protection Bill 2019 (bill),[59] empowers the government to issue an executive order to exempt any government agency from the applicability of the bill. This is applicable when processing of data is necessary for- protecting sovereignty and integrity; security of the state, maintaining friendly relations with foreign states, public order or for preventing incitement to commit cognizable offences.[60] Additionally, compliance with select provisions of the bill has also been exempted, in the cases of investigation, prevention, detection, investigation and prosecution of offences or any other contravention, legal proceedings, domestic purposes and journalistic purposes.[61]

Shortcomings of these Provisions

No legal test: In the *Puttaswamy* Judgment-I[62], the Supreme Court ruled that privacy is not an absolute right, and could be overridden in cases where public interest is more important than individual's interest. In this regard, it empowers the central government to gain access to personal data, subject to satisfying a three-prong legal test of:

1) Legitimacy, to ensure that there is a legitimate aim that necessitates such action by the government;

2) Proportionality, to ensure that action taken by the government is not disproportionate to the aim it is intended to achieve;

3) Legality, to ensure that the abrogation of the fundamental right to privacy should be in accordance with a law.

However, as opposed to the draft bill of 2018[63], this test has been removed from

59 The Personal Data Protection Bill 2019. Available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

60 S. 35 of the bill.

61 S. 36 of the bill.

62 Justice K S Puttaswamy (Retd.) and Another Vs. Union of India and Others SC WP(C) No. 494 of 2012

63 Clause 42 of the Draft Bill of 2018

the bill. It empowers the government to completely exempt any of its agencies from the provisions of the bill, while processing personal data for the purposes mentioned under S. 35. Such exemptions based on a mere executive order, are ultra viers of the *Puttaswamy* judgment II[64], wherein the Supreme Court explicitly stated executive notifications to be insufficient for restricting the fundamental right to privacy. Enabling unaccounted access to personal data to the government without any mechanism for legal checks and balances will not only increase likelihood of privacy violation by the government, but also fuel risks of surveillance, thereby threatening free speech.

No Limitation on Time: Bill does not specify any limitation on the time for which such data can be retained in case of collection for exercise of exemptions. This could increase the chances of data being stored and used by government agencies or data processors beyond the purposes of collection of data in such cases, putting privacy of data principal at considerable risk.[65]

Broad Exemptions: There is a departure in the bill from Draft Bill of 2018[66], which gave exemptions with respect to only certain provisions of the bill such as purpose limitation, collection limitation, consent but still made an exception to ensure fairness and reasonableness in processing and security safeguards. This is specifically relevant to section 35, which gives a broad mandate to government in exempting governmental agencies from the applicability of the entire Bill. Further the exemptions pertain to government agencies.

Recommendations

Reinstating the Legal Test: The three-prong legal test must be reinstated along with specifying that such exemption could only be applied through procedure established by law, for both section 35 and section 36. This legal test is essential to prescribe appropriate substantial and procedural safeguards to maintain the reasonableness and fairness in applying restriction to the fundamental rights.[67] This will also ensure the constitutionality, transparency and accountability by government and its agencies. Additionally, the government should prescribe clear guidelines and provide for

64 Justice K.S. Puttaswamy (Retd) vs Union of India, (2019) 1 SCC 1

65 Justice B.N Srikrishna Committee Report, 2018

66 Clause 42 (2) of the Draft Bill of 2018 "Any processing authorised by a law referred to in sub-section (1) shall be exempted from the following provisions of the Act— (a) Chapter II, except section 4; (b) Chapter III; (c) Chapter IV; (d) Chapter V; (e) Chapter VI; (f) Chapter VII, except section 31; and (g) Chapter VIII."

67 Justice K S Puttaswamy (Retd.) and Another Vs. Union of India and Others SC WP(C) No. 494 of 2012

appropriate judicial order, instead of mandating the exercise of exemption just on the basis of an executive order. We should adopt from the best practices of European Union's (EU) General Data Protection Regulation (GDPR)[68] and Asia-Pacific Economic Cooperation (APEC) privacy framework[69], which also provide for safeguards of necessity, proportionality and as prescribed by the law along with maintaining transparency through public disclosure.

Ensuring Purpose Limitation: The bill should ensure that data is only used with respect to the purpose of exemption, 'purpose limitation' in exercise of exemptions must also be specified. This could be done through stipulating that usage of data must be limited to the purposes of exemptions and that data should only be retained only until the time such purpose is completed and must be deleted thereafter. In this regard, APEC privacy framework also specifies limitations for use only for the objectives of exemptions.[70] Further, the bill should require for the government to conduct a cost benefit analysis to assess if benefits outweigh the cost of exercising exemptions.

Narrowing Exemptions: The bill should limit the scope of exemptions within section 35 by providing the agencies to adhere to provisions relating to notification of breach, offences, penalties, data audits and security safeguards. These are important provisions which protect rights of data principals in cases of misuse of data and helps ensuring transparency.

68 Article 23(1) of the GDPR

69 Part ii (13) APEC Privacy Framework

70 Part ii (13) APEC Privacy Framework

Annexure – D: Data Protection Authority

Background

The Personal Data Protection Bill 2019 (bill)[71] provides for setting up a Data Protection Authority (DPA), while prescribing its composition, functions, powers etc.[72] However, these are plagued with various gaps and unfavourable changes made from its previous draft, as prepared by the BN Srikrishna committee in 2018[73].

Shortcomings in the Provisions

Lack of independence of the DPA: While the DPA will consist of a Chairperson, and upto six whole time members,[74] these shall be appointed exclusively by the central government, while taking recommendations from a selection committee, which shall again comprise of government officials (i.e. a cabinet secretary, and secretaries from the Ministry/Department of Legal Affairs, and Electronics & Information Technology)[75]. With the central government itself being a data fiduciary, there is a clear conflict of interest of the (central government appointed) members of the DPA and the government itself, since it effectively makes the government a judge of its own case, in a situation where the central government is accused of violating any provision of the bill. Furthermore, given the wide discretionary powers of the DPA, excessive central government control over the DPA would effectively enable the central government to hold immense decision-making powers under the bill, which would further weaken the independence and sovereignty of the DPA.

Funds made available through penalties not being used by the DPA: All funds raised from penalties under the bill, are required to be credited in the consolidated fund of India[76], and not in the DPA fund. This results in the removal of the provision of setting up a Data Protection Awareness Fund, as provided for by the previous version of the bill, which was to be maintained through sums realised from penalties.[77] Also, being completely dependent on the central government for its funds,[78] would weaken the independence of the DPA.

Power to make regulations, now shared with the central government: Many powers of the DPA (as granted by the previous draft bill) have been shifted to the central

71 Available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

72 Chapter IX, Sections 41 to 50 of the bill.

73 Available at: https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

74 S. 42(1) of the bill.

75 S. 42(2) of the bill.

76 S. 66(2) of the bill.

77 S. 77(2) of the previous bill.

78 S. 79(1) of the bill.

government. For instance, power to notify additional categories of sensitive personal data are now with the central government, in consultation with the DPA and sectoral regulators.[79] Similarly, there exist irregularity with powers to notify significant data fiduciaries (SDF) which continues to be with the DPA[80], with an inconsistent exception of social media intermediaries, categories of which shall be notified as SDF by the central government[81]. Another such provision is the power of the central government to issue directions to the DPA, to which the DPA would be bound.[82]

Such dilution of powers of the DPA in favour of the central government is not advisable, since the DPA as a regulator would be better equipped with knowledge, experience and information pertaining to data practices, as compared to the central government.

Lack of requirement of transparency in use of discretion: It is to be noted, that despite such sharing of powers with the central government, the DPA still has vast powers to make regulations and the rules to carry out provisions of this bill.[83] However, the DPA has not been mandated to ensure adequate transparency, and not required to undertake cost-benefit analysis (CBA) while framing them.

79 S. 15 of the bill.

80 S. 26(1) of the bill.

81 S. 26(4) of the bill.

82 S. 86 of the bill.

83 S. 94 of the bill.

Recommendations

Adopt an unbiased and neutral selection committee: The selection committee proposed by the previous draft comprised of the Chief Justice of India or a Supreme Court Judge; a Cabinet Secretary; and an expert[84].[85] Such a selection committee appears to be competent, neutral and unbiased, and should be reinstated in the bill. Furthermore, CUTS work on the Draft Regulatory Reform Bill[86] recommends to have one member in the selection committee from a Civil Society Organisation, with experience in consumer affairs or economic regulatory issues.

Also, in order to ensure transparency, a public hearing/consultation on the proposed selection committee must be undertaken before being finalised. Pubic consultations must also provide for inviting candidates it deems qualified to provide their CV's for its consideration, i.e. an open selection process must be adopted, to enable anybody possessing the requisite qualification to apply. Persons working as members or chairpersons in other regulatory commissions may also be invited to apply.

DPA to be a financially independent regulator: In order to ensure the financial independence of the regulator, any revenue generated by the DPA (including from levying

84 Expert having specialised knowledge of, and professional experience in the field of data protection, information technology, data management, data science, cyber and internet laws, and related subjects. Refer S. 50(6) of the previous bill.

85 S. 50(2) of the previous bill.

86 Available at: https://cuts-ccier.org/pdf/CUTS_Comments_on_Regulatory_Reform_Bill-2013.pdf

fines on service providers for violating any provision of the bill) should be deposited under the DPA Fund[87]. Such independent raising of funds could be utilised to meet their expenses as mentioned under S. 79(2), before taking recourse to the Consolidated Fund of India.

Considering that consumer organisations are in a good position to take up the cause of aggrieved consumers and present their case, these funds may also be used to equip them with sufficient and sustained financial resources, in order to ensure that they perform this task of research and advocacy while meeting the appropriate standards. This cause may also be furthered by reinstating the Data Protection Awareness Fund, which may be used to raise awareness and build capacity of users and other stakeholders on issues of/incidental to privacy and data protection.

Shift powers back from the central government to the DPA: CUTS' recommends the shifting of powers (such as the ones mentioned above), from the central government back to the DPA. Decision making by the central government, despite having an expert dedicated regulator would potentially delay decision making, while also fuelling risks of political biasness and conflict of interests.

DPA to adopt scientific regulation making processes: Considering the wide powers given to the DPA (such as those pertaining to issuing codes of practice, classifying data fiduciaries, prescribing standards of data protection etc.), the bill must mandate adopting scientific regulatory decision-making processes, in order to frame optimal regulations, wherein the costs of the regulations do not outweigh its intended benefits. Provisions for undertaking CBA through tools such as Regulatory Impact Assessment[88] must be encouraged in this regard. Conducting competition assessments and/or consulting with the Competition Commission of India, may also be mandated while deliberating on regulations which may impact the market.

87 As provided under S. 79(1) of the bill.

88 Details available at: https://cuts-ccier.org/regulatory-impact-assessment/

Annexure – E: Consumer Grievance Redressal

Background

The Personal Data Protection Bill 2019 (PDPB)[89] empowers data principals (users) to make complaints to data fiduciaries (service providers) in case of any contravention of the bill, which has caused or likely to cause harm to the data principals. It also mandates service providers to have a procedure and an effective mechanism in place to redress such grievances of users, in an efficient and speedy manner (within 30 days of receipt of complaint). Users have also been given a right to approach the Data Protection Authority (DPA), in case they are not satisfied with the relief provided to them by a service provider, pursuant to a complaint.[90]

Furthermore, in case of a personal data breach[91] at the end of a service provider, the bill provides discretion to the DPA, for directing service providers to inform its users about the same, based on an assessment by DPA of the severity of harm likely to be caused to them.[92] It also stipulates security safeguards to be undertaken by the service providers based on associated risk and the likelihood of harm from the processing of data.[93]

Shortcomings of these Provisions

Limitations on Seeking Redressal: No time limit has been prescribed at the level of the DPA as well as the Appellate Tribunal to dispose of any complaints made by users, which may deter them from pursuing their complaints in case of delays in getting their grievances redressed. At the same time, the bill does not provide for a direct remedy to data principals against service providers in

89 The Personal Data Protection Bill 2019. Available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

90 S. 32 of the bill

91 S. 3(29) of the bill states: "personal data breach" means any unauthorised or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to, personal data that compromises the confidentiality, integrity or availability of personal data to a data principal

92 S. 25(5) of the bill

93 S. 24 of the bill

case of offences [94] which limits their avenues for seeking redressal.

Information Regarding Data Breach: By giving sole discretion to the DPA in assessing cases when the users are to be notified of the breach by the service providers, PDPB limits users' information regarding the potential threats to the security of their data. Additionally, there are no specific standards prescribed to assess the 'severity of harm' creating an ambiguity as it may lead to differing interpretations from time to time.

Mechanisms to Seek Remedy: The procedure for seeking remedy must be accessible and understandable to the data principals. CUTS' user perception survey on privacy and data protection[95] had pointed out, that only few users who experienced a personal data breach or a privacy violation, went on to complain about it. Users were also found to be unaware regarding the avenues of registering their grievances.

Limitation in right to seek Compensation: Compensation provision in the PDPB, only gives users' right to claim compensation if they have suffered harm.[96] It limits their rights, as first they will have to make an assessment of the harm suffered and, on that basis, make a claim for compensation. This puts a burden on them to have a complete understanding of harm as prescribed under the PDPB. Further, it does not give any clarification regarding the components of the definition of harm which restricts the understanding of users in assessing harm.

Recommendations

Right to Seek Judicial Remedy: PDPB must empower the court to take cognizance of complaints made by users under Section 83(2), which is now only limited to complaints made by DPA. Provision for such a right to seek remedy has already been emphasised upon by the Supreme Court in the *Puttaswamy* judgment[97] wherein the court stated that limiting such rights might make the remedy seeking mechanism sterile. Additionally, the bill should take on from the best practices from European Unions (EUs) General Data Protection Regulation (GDPR) and the Asia Pacific Economic Co-operation (APEC) Privacy Framework, both of which provide for data principals to seek an adequate judicial remedy. Informed by the Consumer Protection Act 2019, a timeline for not more than sixty days may be provided for resolutions of complaints at the level of both DPA[98] and the Appellate Tribunal.[99]

Notification of Breach (Section 23): PDPB should have a provision for users to be

94 S.83(2) of the bill

95 https://cutsccier.org/pdf/survey_analysis-dataprivacy.pdf

96 S.64 of the Bill

97 Justice K S Puttaswamy (Retd.) and Another Vs. Union of India and Others; SC WP(C) No. 494 of 2012(para 357)

98 S.54 of the bill

99 S. 72 of the bill

notified directly of the data breach by service providers in case of likelihood of harm[100] without undue delay, along with this they should be given recommendations for measures that could be taken to prevent harm. This would help data principals to remain informed and handle their data adequately. Further, it will make service providers more accountable and transparent, which is beneficial for ensuring the trust of users and enhance cyber-security.[101] This practice is also followed in the EU's GDPR and China's Cyber Security Law.[102]

A Mechanism to Seek Remedy: In order to increase the effectiveness of grievance redressal mechanism, the PDPB under Section 50 (Codes of Practice) should prescribe service providers to develop mechanisms for alternate grievance redress options. This could be done through setting up Consumer Service Cells on the lines of CUTS' initiative of *Grahak Sahayta Kendra,*[103] which could act as mediator or conciliator in resolving the complaints. At the same time, consumers should be provided with an easily accessible mechanism to lodge complaints and be updated about the same through the toll-free numbers, online portals (website of the DPA), emails or in person.

Compensation: PDPB should not limit users' right to claim compensation by making it contingent on the harm suffered by them, rather violation itself should be a ground to claim compensation under Section 64. Further, the bill should also provide for more clarification on definitional components of harm so that users are better able to assess the cases of violations that have caused them any harm.

---

100 Chinese Cyber Security Law 2017

101 L. Ablon et al., *Consumer Attitudes toward Data Breach Notifications and Loss of Personal Information. RAND Corporation* (RAND Corporation, 2016).

102 GDPR, Article 34 "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."

103 Consumer Care Centre (Grahak Sahayta Kendra) | CUTS Centre for Consumer Action, Research & Training (CART)," https://cuts-cart.org/consumer-care-centre-grahak-sahayta-kendra/

Annexure – F: Data Localisation

Background

The Personal Data Protection Bill (PDPB) 2019[104], requires explicit user consent, as well as approval of the Data Protection Authority (DPA) or the central government, as the case maybe, and certain conditions being met, for transferring sensitive personal data (SPD) outside the country.[105] Also, a copy of the same is mandatorily required to be stored within the country.[106] Additionally, critical personal data (CPD), which is yet to be defined clearly by the PDPB, has not been allowed to be transferred outside the country, unless for a few narrow exceptions relating to health services or emergency services, or to certain entities outside India only after the approval of the Central Government, if it is satisfied that such transfer does not prejudicially affect the security and strategic interest of the country.[107] Notably, these requirements are a dilution from the Data Localisation (DL) requirements of the Draft Bill of 2018,[108] which imposed local storage of a copy of all personal data.

Shortcomings

Segregation of Types of Data: A substantial portion of SPD is being shared by data principals (users) with different data fiduciaries (service providers) while availing various data driven services. A few instances include financial data being shared with ride hailing apps, food delivery service providers, e-commerce companies and many others. Religious beliefs are being shared with social media platforms, as well as online dating service providers and matrimony websites. Sharing biometric data (finger print scanners and facial recognition software) has become popular amongst consumers for securing their mobile devices from unauthorised use. Given that such SPD is shared in combination with other personal data, it may become burdensome for service providers to segregate the two. This is especially true for smaller service providers, who may not be able to devote adequate resources for such a process, and be compelled to store the entire personal data shared with them, in India, or

104 The Personal Data Protection Bill 2019. Available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

105 Section 34(1) of the Bill

106 Section 33(1) of the Bill

107 Section 34(2) of the Bill

108 Draft Personal Data Protection Bill 2018, available at:

stop serving Indian consumers (particularly in case of smaller foreign service providers, operating in multiple countries).

Additionally, the bill empowers the government to prescribe more categories of SPD and CPD in future under Section 15 and Section 33(2) respectively, without setting clear standards for defining their scope. Also, there is no mention of a timeline for compliance with local data storage requirements of SPD/CPD, which is notified in future. This creates ambiguity for service providers to formulate ways for organising their data, for meeting the localisation requirements under the bill.

Potential Impact of DL on Consumers: A Consumer Impact Assessment study undertaken by CUTS[109] highlighted adverse impact of DL on users in terms of possible reduced uptake of select data-driven services, such as e-commerce, social media and communication services. The study suggests that DL is expected to enhance risks of privacy violation, cyber-attacks and data breaches, while adversely impacting the availability of services and curbing innovation.[110] Hence, while the current bill dilutes certain requirements of DL, there still persists challenges in terms of assessing the effect of DL for SPD and CPD on users.

Possible adverse economic impact: CUTS study 'Digital Trade & Data Localisation'[111] showcased the adverse impact of DL on India's IT-BPM industry, with respect to digital services export. The scope and extent of data restrictiveness may plunge the digital services exports between 10 to 19 percent. This may translate to a shortfall of US$19-US$36bn in achieving the US$1tn economic value potential of the digital sector in 2025. The decline in digital services export will negatively affect the gross domestic product (GDP) by 0.18 to 0.35 percent, causing a shortfall of US$9bn to US$17bn in US$5tn economy objective in 2025.

Recommendations

Regulatory Impact Assessment (RIA): Before taking any decision on prescribing more categories of SPD and CPD, as well as dis/allowing transfer of SPD and CPD, the DPA and/or central government must undertake RIA. Conducting RIA in these scenarios, will ensure that costs imposed by data localisation does not outweigh its intended possible benefits, not only for the consumers but other stakeholders such as service providers.[112] Additionally the findings of such RIA should be published in public domain.

109 Findings available at: https://cuts-ccier.org/pdf/Findings_of_Consumer_Impact_Assessment_of_Data_Localisation.pdf

110 https://cuts-ccier.org/consumer-impact-assessment-on-cross-border-data-flow/the study involved in depth interaction with 40 subject experts, and a survey of over 1200 consumers.

111 Study available at: https://cuts-ccier.org/pdf/project-brief-dtdl.pdf

112 Regulatory Reform Bill

Explore least intrusive means of achieving valid regulatory objectives: The focus of the current bill must remain on upholding privacy and ensuring data protection, and should not be allowed to become a tool for LEA's to access data or propelling economic development. With regards to ensuring regulatory objectives of LEAs the government should strengthen Mutual Legal Assistance Treaties, and pursue international cooperation by becoming a member of 'Chart of signatures and ratifications of Treaty 185: Convention on Cybercrime', or entering into bilateral treaties on the lines of United States Clarifying Lawful Overseas Use of Data (CLOUD) Act. With respect to economic development, encouraging domestic innovation and creating jobs, a separate policy to incentivise processing of data in India may be formulated, instead of forcing DL (as has also been called for in budget 2020)[113].

Strengthen Cross Border Data Flows & adopt best practices: The benefits of cross-border data flows are well documented. In order to encourage the same, India should consider best practices around the world in developing guiding principles for allowing processing of data outside India. The government may consider Asia Pacific Economic Cooperation (APEC) privacy framework[114], APEC Cross-Border Privacy Rules[115] and the recent Digital Economy Partnership Agreement (DEPA) signed between Singapore, Chile and New Zealand, which seeks to enable trusted cross-border data flows between them.

[113] https://www.livemint.com/news/india/govt-s-nudge-may-help-india-become-a-global-data-centre-11580664564132.html

[114] APEC Privacy Framework, 2015

[115] APEC Cross Border Privacy Rules, CBPR

Annexure – G: Overreach of the Bill

Background

In the judgement of K.S. Puttaswamy vs. Union of India, 2017,[116] the Supreme Court of India (SC) recognised 'right to privacy' as a fundamental right. '***Recognizing the importance of data protection and keeping personal data of citizens secure and protected***'[117], Ministry of Electronics and Information Technology (MeitY), The Government of India (GoI) had formed a committee (led by retired justice BN Srikrishna) to '***study and identify key data protection issues and recommend methods for addressing them***'[118], which proposed the draft Personal Data Protection Bill 2018 (draft bill)[119]. The committee also came out with a detailed report which recognised the objective of the draft bill to be '***to unlock the data economy, while keeping data of citizens secure and protected***'. After a round of public consultation, The Personal Data Protection Bill, 2019 (bill)[120] was introduced in Lok Sabha, with certain changes to the previous draft.

The Statement of Objects and Reasons of the bill explicitly states the object of the bill to '***bring a strong and robust data protection framework for India and to set up an Authority for protecting personal data and empowering the citizens' with rights relating to their personal data ensuring their fundamental right to "privacy and protection of personal data***''.

Overreach of the Provisions

While the preamble of the bill enlists various necessary facets of a personal data protection regime, a few issues have been included in it, which are beyond the objects and reasons given for the bill. These pertain to 'laying down norms for social media intermediary'; and 'ensuring empowerment, progress and innovation through digital governance'. Notably, these are new additions made from the previous draft bill, which have now been proposed in relevant provisions under the revised bill, and have been discussed below.

116 Justice K S Puttaswamy (Retd.) and Another Vs. Union of India and Others; SC WP(C) No. 494 of 2012 – judgement delivered on August 24, 2017

117 https://pib.gov.in/newsite/PrintRelease.aspx?relid=181928

118 https://pib.gov.in/newsite/PrintRelease.aspx?relid=169420

119 https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

120 http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

GoI's access to non-personal data and anonymised personal data: The bill empowers the GoI to get access to non-personal data, or anonymised personal data processed by service providers (data fiduciaries), for select regulatory objectives.[121] However, such a provision appears to be beyond the scope of the bill, since the same has been restricted to '***personal data***' as mentioned above. The provision also runs the risk of overlap with a separate committee chaired by Kris Gopalakrishnan, which is deliberating on framing governance norms for non-personal data.[122]

Also, forced access to non-personal data may infringe intellectual property rights of service providers pertaining to such data. Retired justice BN Srikrishna has also raised concerns to this effect. He recently mentioned - '*through this clause, the government can access all business data, including data on intellectual property, business strategy and mergers & acquisitions*', which he felt was dangerous.[123]

Voluntary verification of users of social media intermediaries: The bill empowers the GoI (in consultation with the Data Protection Authority) to notify certain social media intermediaries[124] as significant data fiduciaries,[125] who would need to provide its users with voluntary account verification options,[126] and provide a visible mark of verification to those availing such an option[127]. As was the case with the above provision, this also appears to be beyond the contours of '***personal data protection***', and hence this bill.

User verification intuitively seeks to solve the problem of inappropriate posts/information through this legislation, which may be considered an overreach, since the issue is already being deliberated upon in The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018.[128] CUTS in its submission of comments on the same, flagged how the provisions of the amendment rules are antithetical to privacy and anonymity, and also highlighted the

121 S. 91(2) of the bill.

122 https://www.medianama.com/2019/09/223-meity-non-personal-data-committee/

123 https://economictimes.indiatimes.com/tech/internet/govt-exemptions-in-personal-data-protection-law-can-be-challenged-in-court-says-justice-srikrishna/articleshow/73762019.cms?from=mdr

124 "social media intermediary" is an intermediary who primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services, but shall not include intermediaries which primarily,— (a) enable commercial or business oriented transactions; (b) provide access to the Internet; (c) in the nature of search-engines, on-line encyclopedias, e-mail services or online storage services. S. 26(4) of the bill.

125 S. 26(4) of the bill.

126 S. 28(3) of the bill.

127 S. 28(4) of the bill.

128 https://meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf

various compliance costs it may impose on service providers.[129]

Recommendations

Remove such provisions from the bill: Considering such overreach of the provisions, it is recommended that these be removed from the bill. Risks of regulatory overlaps must also be avoided, given the overriding effect of the bill.[130] Notably, the GoI shall still retain power to chase its regulatory objectives through other appropriate legislations, since it has explicitly been empowered to frame policies pertaining to digital economy, including measures for its growth, security, integrity, prevention of misuse, which are beyond the ambit of personal data.[131]

Adopt scientific regulatory making processes: Even while being pursued in other legislation (after being removed from the bill), it is imperative to adopt a scientific regulation making process by conducting Cost-Benefit Analysis of proposed regulations, in order to ensure that the costs of the regulation, do not outweigh its intended benefits. Evidence-based policy making tools, such as Regulatory Impact Assessment (RIA)[132] may be useful in this regard, which help in balancing interests of all stakeholders during policy making.

129 https://cuts-ccier.org/pdf/CUTS_comments_on_the_Information_Technology_Intermediary_Guidelines.pdf

130 S. 96 of the bill.

131 S. 91(1) of the bill.

132 https://cuts-ccier.org/regulatory-impact-assessment/

Annexure – H

Introduction

As countries increasingly realise the value of data for their economy and recognise the importance of protecting it, they are beginning to develop their regulatory frameworks on privacy, data protection, and related issues. More often than not, such frameworks have unique features informed by the respective country's vision of digitalisation and the use of digital services for its economy. India is no exception. While India's Personal Data Protection Bill 2019 (PDPB), borrows from the European Union's (EU) General Data Protection Regulation (GDPR), it also has certain unique features. It is, therefore, pertinent to compare and contrast some key features of different privacy and data protection legislation, including PDPB and GDPR, to better understand the intent and objectives of different countries. Such comparison becomes even more pertinent as data governance cannot be a solely territorial concept and seamless data flow across jurisdictions is critical to leverage its value and essential for realisation of the vision of the digital economy and growing tech industry in many countries.

Comparison Matrix

The matrix below compares certain key features: a) the GDPR framework which is considered one of the most comprehensive data protection framework in the world; b) Asia Pacific Economic Cooperation (APEC) Privacy Framework, which aims to enhance cross border data flows amongst members of APEC, without compromising on standards of privacy and data protection; c) China, which is one of the biggest data regimes focusing on state control over data flows, with its recent adoption of the Cyber Security Law; d) Japan's Act of Protection of Personal Information (APPI), which is now considered to be amended to align with GDPR; e) California Consumer Protection Act 2020, through which California became the first US state to have a specific data protection law and is being called GDPR 'lite'; and f) India's PDPB 2019, which is now under the consideration of Joint Parliamentary Select Committee.

Country	General Data Protection Regulation- EU 2018	APEC Privacy Framework 2015	Chinese Cyber Security Law 2017	Japan's Act of Protection of Personal Information 2017	California's Consumer Privacy Act of 2018	India's Personal Data Protection Bill 2019
Definition of personal data and the segregation between categories of data	Personal data means any information relating to an identified or identifiable natural person ('data subject'), and means any information that can directly or indirectly identify a person.	Personal information is information that can be used to identify an individual. It also includes inferences drawn from such information. **There is no differentiation between**	Personal data refers to various information that is recorded in electronic or other forms which can be used to identify a person. The law does not itself prescribe any definition of the sensitive personal data although	Personal information includes any information that makes a person identifiable. **Sensitive personal data is defined as data that needs to be handled carefully so as to not cause discrimination**	Personal data is referred to as personal information that can identify a person and includes inferences drawn from such information. **No separate category for sensitive**	Personal data is defined as data through which a person can be identified, both online and offline, directly and indirectly, and include inferences drawn for profiling. **Sensitive data includes financial data but does not**

Country	General Data Protection Regulation- EU 2018	APEC Privacy Framework 2015	Chinese Cyber Security Law 2017	Japan's Act of Protection of Personal Information 2017	California's Consumer Privacy Act of 2018	India's Personal Data Protection Bill 2019
	Sensitive data does not include financial data and passwords.	**personal and sensitive personal data.**	standards provide for it as **data which if divulged can lead to person, property, psychological harm or discrimination. It includes information related to bank accounts.**	**and prejudice and does not include financial data and passwords.**	**personal data**.	**include passwords.** The government is authorised to notify categories of personal data as sensitive personal data having regard to the risk of significant harm on processing and expectation of confidentiality with such data.
Processing of Data	Processing of data must be done in a lawful, fair and transparent manner, only for an explicit and **legitimate purpose and no further processing which is**	The processing of the data should be lawful and fair. **The data should only be used for the purposes of collection as informed to the user while collection and other**	Processing of data should be lawful, justifiable and necessary. It further explains the **meaning of lawful, i.e. to not deceive, force or inveigle the data subject. It also provides for the 'clear purpose**	There is no specific provision for transparency and requirements of fairness and reasonableness, although **data subjects must be informed about the utilisation of their data.**	Businesses have the responsibility to **inform the consumer about the purpose of collecting and the information should be used for that purpose only**. It is the responsibility of	Data has to be processed in a fair and reasonable manner for the purpose for which it has consented **which includes an incidental purpose or the purpose which is connected to the**

Country	General Data Protection Regulation- EU 2018	APEC Privacy Framework 2015	Chinese Cyber Security Law 2017	Japan's Act of Protection of Personal Information 2017	California's Consumer Privacy Act of 2018	India's Personal Data Protection Bill 2019
	incompatible with that purpose.	**compatible purposes. The framework gives examples of such compatible purposes**	**principle' for the processing of data**.		the business to provide an opt-out option if the consumers do not wish to share the information.	**initial purpose.**
Exemptions from data protection	Exemption for defence, national security, for conviction of offences and general public interest. **Such use includes the condition of necessary and proportionate to the purpose for which the data is used.**	Exemptions are provided for in the case of security, sovereignty, safety, and public policy, **although it provides for conditions of limited and proportionate use and authorised by the law and should be made known to the public.**	Exemptions are public interest, law enforcement purpose, national security, the voluntary publication of information by an individual. The law also gives power to the government to demand data from network operators in the case of an emergency. **No legal test for proportionality.**	Exemptions are uses required by law, preventing bodily harm, to improve public health. **No principle of proportionality**.	The exemption relates to the compliance of the business with laws, judicial proceedings, criminal proceedings and cooperating with public authorities for the matter of enforcement of the law. **No particular legal text specified.**	The government may for national security or public interest considerations exempt its agencies from any provision with respect to data protection. Exemptions also exist for the processing of personal data for legal or judicial purposes. **No condition of legality, necessity and**

Country	General Data Protection Regulation- EU 2018	APEC Privacy Framework 2015	Chinese Cyber Security Law 2017	Japan's Act of Protection of Personal Information 2017	California's Consumer Privacy Act of 2018	India's Personal Data Protection Bill 2019
						proportionality for applying for exemptions.
Non- Personal Data and Voluntary Verification by Social Media Intermediaries	GDPR specifically focuses on personal data protection and **does not provide for usage of non-personal data/ information** and does **not provide for voluntary verification provisions** for social media intermediaries	With the aim of promoting information flows **only focuses on the uses of personal information**. There is **no requirement of voluntary verification** by social media intermediaries	It provides for cybersecurity and privacy provision with respect to **personal information and does not include non-personal data. It does not include the provision for voluntary verification**	It **only focuses on personal data; usage of non-personal data is not included** within the law. There is **no requirement for voluntary verification** by social media intermediaries.	**It only covers personal data of consumers** there are no provisions regarding the non-personal data. There is **no requirement of voluntary verification** by social media intermediaries.	The law **provides for the transfer of non-personal data to the government in certain cases** and requires social media intermediaries to **give provisions for voluntary verification of users.**
Data localisation and data flows	Allows for data flows, and allows for data storage in **GDPR compliant locations.**	Promotes cross border data flows with companies and countries which are **compliant with the APEC**	The requirement of data localisation and cross border **data flow is only permitted after consent and establishment of**	**Data transfer is allowed after the consent of the data subject**. Although such consent is not required if the	**Transfers are not restricted**, although transfers to the service provider, requires compliance with data protection	**Data localisation not applicable except in cases of sensitive personal data and critical personal data**, which can be

Country	General Data Protection Regulation- EU 2018	APEC Privacy Framework 2015	Chinese Cyber Security Law 2017	Japan's Act of Protection of Personal Information 2017	California's Consumer Privacy Act of 2018	India's Personal Data Protection Bill 2019
		privacy framework.	**appropriate business needs.**	other **country is considered data protection compliant**. Example- EU	provisions within the legislation.	transferred outside after approval from the data protection agency or the government, as the case may be.
Consent Mechanisms	Consent should be informed, free, capable of being withdrawn and demonstrable**.**	Where appropriate, individuals should be provided **with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information.**	Provides for consent requirements for lawful processing. **Although does not mention specific modes or mechanism** for obtaining consent.	For the purpose of processing the data, consent is required. **Although there is no prescribed mechanism for obtaining consent**	Consumers need to be informed about the purpose of collection of data and they should **provide consumers with an opt-out option if they font wish to share data.**	Provides for clear, specific, informed consent capable of being withdrawn. It provides for the **mechanism of consent managers** through whom consent can be provided and withdrawn.

Country	General Data Protection Regulation- EU 2018	APEC Privacy Framework 2015	Chinese Cyber Security Law 2017	Japan's Act of Protection of Personal Information 2017	California's Consumer Privacy Act of 2018	India's Personal Data Protection Bill 2019
Rights of data subjects/ principals	Right to be forgotten, right to restrict processing, right of data portability (by automated means), **right not be subject to automated processing**	Right to access and correction, the right to be informed about the data transfers	Right to access data, right to rectification of errors, right to deletion /forgotten, right to object processing, right to restrict processing, right to portability is specified cases, right to withdraw consent, **right to object marketing, right to complain to the authority**	Right to access, **correction, data portability**, rectification of errors, right to object processing, **right to restrict processing**, right to withdraw consent, right to object marketing, right to complain	Right to view and access data, right to erasure, right to opt-out from sharing of data, right to stop companies from selling data, limited recognition of the right to portability	Right to confirmation and access, correction and erasure, data portability and forgotten. The data principal needs to make a request in writing to exercise the rights, and the data fiduciary may charge a fee to comply with certain requests.
Authority for Implementation	Specifically provides for setting up of **independent authority by member states for the implementation of the GDPR**. It specifically	The framework gives member states to autonomy to formulate authority for **enforcement through central authorities, multi-agency**	**The law does not provide for any specific authority** or regulator rather the powers are distributed amongst various government departments.	**Independent Personal Information Committee (PPC)** is being set up for the implementation of the act, which also provides for collaboration with other sector-	**There is no independent authority** for enforcement and implementation of the act.	The law provides for setting up **of Data Protection Authority (DPA) without any independent members, to be nominated by a selection committee**

Country	General Data Protection Regulation- EU 2018	APEC Privacy Framework 2015	Chinese Cyber Security Law 2017	Japan's Act of Protection of Personal Information 2017	California's Consumer Privacy Act of 2018	India's Personal Data Protection Bill 2019
	provides that **such authority must not be influenced by external factors and would have complete financial and administrative autonomy in exercising its functions.**	**enforcement bodies, a network of designated industry bodies, or a combination of the above, as Member Economies deem appropriate**.		specific ministries.		**comprising government representatives**.
Penalties	**Provides for administrative fines and penalties based on the level of damage suffered by the data subject.** Although such fines differ on the basis of specific infringements, with the highest	Encourages member states to adopt an appropriate framework to deal with threats and breaches. It provides for member stated to come up with remedies which are commensurate to	Provides for penalties in case of infringement and specifically also provides for a person responsible along with revocation of business licence. **Provides for criminal sanctions in cases where network**	Both imprisonment and fine. **The highest penalty which includes both fines imprisonment in the cases of uses of the personal database for unlawful gains.**	**There is a right for private action, provides for penalties**. The fines are decided according to the damages suffered	Penalty and criminal sanctions for up to three years in certain cases. **Criminal penalties are provided in the cases where the personal data is re-identified without consent of data fiduciary**. Penalties are

Country	General Data Protection Regulation- EU 2018	APEC Privacy Framework 2015	Chinese Cyber Security Law 2017	Japan's Act of Protection of Personal Information 2017	California's Consumer Privacy Act of 2018	India's Personal Data Protection Bill 2019
	fines for infringement related to processing, consent and rights of data subjects and overhaul of data protection's authority. It emphasises that such penalties or fines imposed must be effective, proportionate and dissuasive.	the degree harm due to the violation.	**managers refuse to make rectifications after being notified for three years**.			imposed only if the adjudicating officer considers there is infringement or harm caused as provided under the act and based on the degree of the harm caused.
Grievance Redress	GDPR gives the right to data subject to lodge complaint both to the supervisory authority and **gives right to claim appropriate judicial remedy**	Encourages member states to come up with their own frameworks which maybe include the **right of individuals to pursue legal actions or**	Provides **for the right to make a complaint to authorities which include Cyberspace Administration of China (CAC), telecom authority and the public**	Provides for the right to lodge a complaint about **data breaches to the Personal Information Protection Committee**. There is no right to lodging a complaint	**Consumers have the right to initiate a civil action in the courts** pursuant to their rights being violated in case of a data breach.	Provides for the right to data principal to **lodge a complaint about breach of rights and non-compliance by data fiduciaries to the Data Protection**

Country	General Data Protection Regulation- EU 2018	APEC Privacy Framework 2015	Chinese Cyber Security Law 2017	Japan's Act of Protection of Personal Information 2017	California's Consumer Privacy Act of 2018	India's Personal Data Protection Bill 2019
	in case their rights are violated under the regulation	**industry self-regulation.**	**security authorities and other concerned authorities**. Although it does not provide for lodge the complaint to the court itself.	to the court.		**Authority (DPA). It does not provide for the right to data principal to lodge the complaint directly to the court.**
Obligations of Data Fiduciaries/ Controllers	**Data controllers are to report the data breaches to the data subjects in cases where there is a high risk of breach** of rights of data subjects. If the data controller fails to do so the supervisory authority must inform the data subject of the same.	Gives flexibility to member states to adopt mechanism which ensured accountability of controllers to maintain appropriate security for breaches and provide necessary remedies to the individuals	**It obligates the network operators to report the data breaches to the data subject in a clear language** indicating the nature of the breach and also suggestion to mitigate the breach and also to the concerned authority.	**The law states that it is preferable for handling operator to inform the data subject** of the breach so that they can take appropriate mitigating measures.	**There is no provision of reporting breaches**, but the consumers have the right to access information related to any data transfers and give business notice of 30 days if there is any breach.	The obligation of the **data fiduciary to report the data breach to the data principal rests on the discretion of the Data Protection Authority (DPA)** based on the severity of the harm and the requirement of mitigating responses by the data subjects.

Conclusion and the Way Forward

Through the comparison matrix, it can be inferred that GDPR is focused in its approach towards enshrining privacy and data protection as key rights for users. China has its own unique approach, while the APEC framework has established principles for data flows and protection. At the same time, California takes a narrow approach to protection targeting only specific kinds of processing.

GDPR gives a broad definition of personal data and has a separate category for sensitive personal information much of what is reflected in India's proposed PDPB. However, India goes a step further by authorising the government to specify categories of personal data as sensitive. Other jurisdictions broadly recognise sensitive information as information which might result in discrimination or cause harm, thus providing clear principle/ rationale for classification.

While most jurisdictions recognise the exemption from data protection provisions for law enforcement and judicial purposes, GDPR provides for the principle of necessity and proportionality which is absent from the PDPB, which authorises the government to exempt any government agency.

With respect to cross border data flows, while GDPR allows comparatively free data flow to adequately compliant countries, this is in contrast with China's framework which adopts for localisation requirement. APEC framework in this regard is specifically notable as it establishes principles for protection and data flows considering a balanced approach and leaves it on individual states to still frame their own laws based on certain principles as enshrined within APEC framework. Japan is also trying to move towards such a balanced approach by allowing transfers with equally compliant countries. India, however, appears to be providing a lot of discretion to the government and the data protection agency to allow or prevent cross border data flows, without any guiding principles in this regard.

With regard to consent mechanisms, apart from the principles of free, clear, legitimate consent which are similar to that of GDPR, India's law is a step ahead and provides for consent managers as a separate set of data fiduciaries to provide and withdraw consent. However, it needs to be ensured that such data fiduciaries do not end up becoming gatekeepers of consent. India can also learn from APEC framework which requires consent mechanisms to be easily understandable, accessible and affordable. In relation to rights of data subjects and penalties thereof, GDPR has a broad framework that gives complete control of data within the hands of the consumer while APEC privacy framework and California Consumer Protection law have more limited rights. While the

PDPB provides several rights, it should include the right to restrict processing and right against data processing.

It is necessary to ensure consistency among individual data protection regimes to give shape to a global data governance regime, for fostering data flows and leveraging the value of data and ensuring optimum data protection for the users. This is especially important for an economy such as India, which has second-highest internet users after China and immense potential for the growth of the digital economy. While the government is considering frameworks for non-personal data as well as personal data it will be pertinent to take an approach of reviewing laws from other jurisdictions and reflect on best practices. This will help in designing optimal provisions that can enhance protection and at the same time foster growth of the digital economy.

In lieu of the above, following proposed in the PDPB 19:

- **Definition of Sensitive Personal Data (section 3(36))** – Informed by the Japanese and Chinese frameworks, a guiding principle could be adopted in section 2(36) for considering **such personal data as sensitive personal data, unauthorised use of which could lead to physical, property, or psychological harm to data principals**. In addition, passwords should be inserted in the list of sensitive personal data as it is considered as a data protection tool by users as validated by CUTS consumer perspective study on privacy, data protection and data sharing.
- **Classifying Personal Data as Sensitive Personal Data (section 15)** – To avoid confusion and ensure clarity, the terms 'significant harm' in section 15 should be replaced with 'physical, property or psychological harm'. In addition, for promoting transparency, competitive neutrality and preventing abuse of discretion, **the government must be required to undertake cost-benefit analysis and release its findings in public domain while proposing alteration in the definition of sensitive personal data.** As a result, it will need to justify that the benefits of classifying a set of personal data as sensitive personal data while excluding other similar sets of personal data outweigh the costs of such action.
- **Purpose limitation (section 5(b))** – At present, data fiduciaries are allowed to process the personal data for purposes that are 'incidental to' or 'connected with' the purpose consented to by the data principal. The use of such terms leaves a lot of ambiguity. Informed by the APEC and GDPR framework, these terms should be replaced with **'purposes compatible with such purposes' to ensure direct linkages between consent provided by the data principal and purpose for which the data is processed.** While ensuring data protection, this will also

promote innovation. The legislation may also provide examples of compatible purposes, as provided in the APEC framework.

- **Exemptions (section 35)** – Much like the GDPR, and in compliance with the *Puttaswamy* judgment, the PDPB should require the **government to justify that the order exempting its agency from PDPB complies with the principles of legality, necessity, and proportionality.** In this regard, the **government must be required to undertake a cost-benefit analysis and release its findings in the public domain** to justify that the costs of its action are outweighed by the benefits.

- **Data Flows (section 33 and 34)** – To promote transparency and avoid abuse of discretion, **while notifying critical personal data** under section 33, the **government should be required to undertake cost-benefit analysis** and release its findings in public domain to justify that benefits of its action outweigh the costs. Similarly, **while making a decision under section 34(2)(b)** on whether a transfer prejudicially affects the security and strategic interest of the state, **the government should be required to undertake cost-benefit analysis** and release its findings in public domain to justify that benefits of its action outweigh the costs. In addition, the government should adopt principles from GDPR, APEC and Japanese frameworks to pre-approve transfers of data to jurisdictions adopting high-quality data protection standards. The government should also enter into bilateral and multilateral partnerships for ensuring cross-border data flows.

- **Notice (section 7(2)) –** While the PDPB provides that the notice under section 7(2), is concise and easily comprehensible to a reasonable person and in multiple languages where necessary and practicable, based on APEC privacy framework, **principles of easy accessibility and affordability of notice should also be adopted** in section 7(2).

- **Data Protection Authority (section 42)** –PDPB prescribes formulating a selection committee for setting up the DPA which consists of the members of the executives of the government, hence, it comprises the independence of the functioning of the regulatory body through an indirect oversight of the executive. **Both GDPR and Japan's APPI provides for an independent regulator for the implementation of the provisions of the legislation through specifically providing administrative and financial independence and that such authority should not be directly or indirectly influenced by external factors.** Considering that India should reconsider the independence of the regulator with respect to current provision, and should include members of the judiciary, experts in data protection and civil society members in the selection

committee to ensure its administrative and financial autonomy along with members of the executive.

- **Non- Personal Data and Voluntary Verification by Social Media Intermediaries (section 91 and 93)**- PDPB Provides for transfer of non-personal to government in certain cases for policy-making or delivery of services and provides for voluntary verification**, both these provisions are not within the scope this bill as this bill specifically focuses on personal data protection**. No such provisions are provided in any other privacy law in other jurisdictions; hence these provisions must be removed from the bill.
- **Grievance Redress (Chapter V and Section 83)** – In the current form, PDPB limits the right of data principals as it restricts the power of the courts to only take cognizance of the offence when the complaint is made by the DPA**. In order to give more powers to data principals regarding handling of their data, the data principal must be given the right to seek adequate judicial remedy in case of data breach and infringement of their rights under Chapter V which provides for rights of data principals and under section 83** as is also provided in the GDPR, APEC privacy framework, and California Consumer Privacy Act.
- **Penalties (Chapter X) -** PDPB prescribes criminal sanctions and fines in the case of re-identification of the data without consent, although for other breaches penalties are only provided after the assessment by the inquiry officer regarding harm and violation. Like **the GDPR, the PDPB must include a guiding principle regarding the fines to be effective, dissuasive and proportionate to the harm caused within Chapter X which is focused on deciding penalties.**
- **Information regarding Data Breach (section 23)** - GDPR, China's Cyber Security Law and Japan's APPI provides for data subjects to be informed about the harm in the case of data breaches. **PDPB should require data fiduciaries to notify the data principals of the breach in case of the likelihood of harm and give directions of mitigating such harm under section 23** as provided under China's Cyber Security law**.** This will give broader protection to the data principals.

References

1. *General Data Protection Regulation (EU) 2016/679 (GDPR)*
2. *APEC Privacy Framework (2015)*
3. *Cyber Security Law of People's Republic of China, Standing Committee of the National's People's Congress (2017)*
4. *Act on Protection of Personal Information 2003, Government of Japan (2017)*

5. *California Consumer Privacy Act of 2018 (2020)*
6. *Personal Data Protection Bill, Government of India (2019)*
7. Wie Sheng, "One Year after GDPR, China Strengthens Personal Data Regulations, Welcoming Dedicated Law · TechNode," *TechNode* (blog), June 19, 2019, https://technode.com/2019/06/19/china-data-protections-law/.
8. Torre, Lydia. "GDPR Matchup: The California Consumer Privacy Act 2018."https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/.