# REPORT ON 'COMMENTS TO THE PERSONAL DATA PROTECTION BILL, 2019'


## PREPARED BY

AGNIDIPTO TARAFDER (FACULTY ADVISOR)

SIDDHARTH SONKAR (COORDINATOR)

ROHIT GUPTA

AKSHAY LUHADIA

ASEES KAUR

SWARNA SENGUPTA

ON BEHALF OF,

**THE KAUTILYA SOCIETY,**

**NATIONAL UNIVERSITY OF JURIDICAL SCIENCES (NUJS), KOLKATA**

# INTRODUCTORY ADDRESS FROM

# THE KAUTILYA SOCIETY, NUJS

To,

Mrs. Meenakshi Lekhi,

Member of Parliament & Chairperson,

Joint Parliament Committee,

Personal Data Protection Bill, 2019,

Lok Sabha.

Dear Ma'am,

We write to you on behalf of the Kautilya Society, a collaboration between students of National University of Juridical Sciences (NUJS), Kolkata and Vidhi Centre for Legal Policy, New Delhi. Student members of the Kautilya Society seek to actively participate in legislative processes to help in the making of better laws and to cultivate an interest in participating in legislative research and policy-making. To this effect, we have endeavored to undertake a critical study of the Personal Data Protection Bill, 2019 ('the Bill') and attached herein our comments and suggestions to the same in the nature of this Report.

The first part of this Report contains the Executive Summary, i.e. a glance-through of all the recommendations in this Report. The second part contains a detailed explanation of the various recommendations we make based out of justifications in law and policy. In the Executive Summary, we have summarized a few concerns which have already been raised by other stakeholders. We have not included these concerns in the second part, which contains the detailed explanation.

We realized that several stakeholders have already reached out to you with respective comments. While writing this report, we have tried our best to not raise concerns which have already been raised earlier. However, we felt that it is necessary to summarily flag concerns with respect to a few provisions which continue to remain in the final draft of the Bill.

We sincerely hope that the Joint Parliamentary Committee gives us an opportunity to appear before it to justify the need to consider the inclusions and modifications we have suggested in this Report. We also hope that the Joint Parliamentary Committee actively considers the recommendations that we make in this Report while finalizing the Bill.

Sincerely,

Kautilya Society,

National University of Juridical Sciences (NUJS), Kolkata.

# TABLE OF CONTENTS

**I. EXECUTIVE SUMMARY ..... 4**

**II. SUMMARY OF STAKEHOLDER RECOMMENDATIONS ..... 7**

**III. DETAILED COMMENTS ..... 9**

A. POWER TO NOTIFY CRITICAL PERSONAL DATA ONLY WITH CENTRE ..... 9
B. NO GUIDING EXPLANATION IN NOTIFYING CRITICAL PERSONAL DATA ..... 9
C. ALGORITHMIC TRANSPARENCY AND EXPANDING THE RIGHT TO CONFIRMATION AND ACCESS ..... 10
D. INDEPENDENCE OF CONSENT MANAGERS FROM THE DATA FIDUCIARY ..... 10
E. FIDUCIARY DUTIES ..... 12
F. EXCLUDING ANONYMISED PERSONAL DATA FROM SECTION 91 ..... 12
G. LIABILITY FOR JOINT CONTROLLERS MISSING: TAKING FROM THE TRUST ACT ..... 13
H. INDEMNITY CONTRACTS AGAINST PENALTIES FOR BREACHING OBLIGATIONS UNDER THE BILL MUST BE EXPRESSLY PRECLUDED ..... 14
I. LEGACY DATA ..... 14
J. SECTION 19 ..... 15
K. SURVEILLANCE ..... 16
*a. Definition of Surveillance ..... 16*
*b. Procedure and Preconditions for The Grant of an Order for Surveillance ..... 17*
*c. Admissibility of Unconstitutionally Obtained Evidence ..... 18*
*d. Rights Of Data Principals Subject To Surveillance ..... 18*
L. WITHDRAWAL OF CONSENT ..... 19
*e. Requirement of a Valid Reason ..... 19*
*f. Consequences of Withdrawal of Consent ..... 19*
M. REGULATORY SANDBOXES ..... 19
*g. Selection Criteria and Regulatory Regime ..... 19*
*h. Deletion of Data Upon Expiry of Sandbox Duration ..... 20*
N. FAILURE TO PROVIDE A REASONABLE EXPLANATION UNDER SECTION 58 ..... 20
O. CONSULTATION V. CONCURRENCE UNDER SECTION 15 ..... 21
P. RIGHT TO BE FORGOTTEN ..... 22
Q. THE DATA LOCALIZATION CONUNDRUMS WITHIN THE PURVIEW OF INDIA ..... 22

**IV. VISION FOR THE FUTURE: INCREASING DIGITAL LITERACY INITIATIVES ..... 24**

# I. EXECUTIVE SUMMARY

***Apportion* Power to Notify Critical Personal Data**: The power to notify critical personal data remains only with the Central Government, as compared to the power to notify protected systems under the Information Technology Act, 2000 ('IT Act'), which specifies appropriate government. We recommend that states, in matters which fall within List II, should also have the power to notify critical personal data (such as in the context of state employees, land records, etc). This would be in conformity with the federal structure of the constitution.

***Include* Guiding Principles to Notifying Critical Personal Data**: An explanation containing principles which would guide the Central Government in notifying critical personal data similar to the one under the IT Act should be included.

***Include* Right to Access Algorithmic Guiding Principles**: The right to access should include the right to access the guiding principles driving the processing of personal data. This would increase algorithmic transparency in government use of artificial intelligence in public delivery systems.

***Increase* Regulations for Consent Managers**: At present, consent managers are only subject to registration and few other obligations under the Bill. We feel that privacy obligations under the Reserve Bank of India's ('RBI') Master Direction on account aggregators should at the very least be imported to consent managers. In addition to these obligations, consent managers must also not carry on any business other than that of consent management. Consent managers must also not be parties related to the data fiduciary responsible for processing the personal data of a data principal in a given situation.

***Exclude* anonymised personal data from section 91:** Presently, the Bill allows the Government to require data fiduciaries to share anonymised personal data with the Government. There is no globally recognised standard of anonymisation which can make reidentification impracticable at any point in time. So, we recommend that the power of the Government be limited to non-personal data only (example, geospatial data), excluding from its scope, the power to share anonymised personal data.

***Include* Legacy Data**: Presently, once an individual faces demise, it is unclear what occurs with their personal data. We recommend in this field that a person whilst alive should be given the opportunity to choose another person who, upon his passing, will be the legacy data principal. The legacy personal data shall have access to the data principal's data, the right to erase his data and furthermore has the ability to refuse further processing of the data principal's data.

***Incorporate* the Test of Proportionality within Section 19 of the Bill**: Section 19 gives certain rights to the data principal in regards to his data being processed through automated means. Although, Section 19(2) of the Bill gives wide discretion to the Government to disregard the element of consent. It is recommended that the '*Test of Proportionality*' be incorporated in the conferral of such powers.

***Address* the Issue of Surveillance**: While the Bill defines both surveillance and observation as forms of harm, it fails to lay down a definition for the same. In light of recent debates questioning the authority and manner of granting an order for surveillance, it is recommended that the terms be defined and a subsequent framework of judicial oversight be adopted in order to ensure accountability and transparency. Further, it is imperative that the data principal possess a right to

challenge the order for surveillance upon being notified of the same. Lastly, the admissibility of evidence collected *sans* the judicial/executive sanction to do so is revisited in light of recent jurisprudence concerning the fundamental right of privacy and its implications thereof.

***Clarify* the Conditions for Withdrawal of Consent**: While the data principal is free to give consent to the processing of data by a data fiduciary, there is an additional requirement of providing a '*valid reason*' for the withdrawal of such consent. Since the data principal itself is bearing the cost of such a withdrawal, in that some services provided by the data fiduciary may be withheld, it is unclear why such a requirement for the withdrawal of consent exists. Additionally, Section 9(6) of the Bill fails to identify the legal consequences bearing out of such an unjustified withdrawal. There is a need to clarify the same.

***Standardize* the Regulatory Sandboxes Regime**: The Regulatory Sandbox regime proposed by the Bill deviates from that established by the RBI in the context of Financial Technology. In doing so, it ignores some of the important safeguards identified and incorporated within the same in order to protect the interests of consumers participating in the experimental environment. Thus, it is recommended that the regime be standardized or, in the alternative, stronger safeguards, relating to the qualification of those eligible to participate in the Sandbox, be incorporated.

***Qualify* the Requirement to Provide a Reasonable Explanation Under Section 58 of the Bill**: Article 58 of the Bill requires data fiduciaries to furnish a '*reasonable explanation*' in case it fails to comply with its obligations under Chapter V of the Bill. Since the Bill does not qualify what exactly constitutes a '*reasonable explanation*', it is our suggestion that the same be defined in terms of Article 19 of the Constitution.

***Include* Concurrence Under Section 15 of the Bill**: Under Section 15 of the Bill, the Central Government may, in consultation with the Data Protection Authority ('the Authority'), notify categories of personal data as 'sensitive personal data.' It is recommended that the word 'consultation' be altered to 'concurrence' for better autonomy and functioning of the Data Protection Authority.

***Amend* Right to be Forgotten -** Under the Bill, if a data principal wants to exercise his '*Right to be Forgotten*', the data principal must make an application to the Adjudicating Officer. The data principal must also show why his right to be forgotten is higher than the Data Fiduciary's right to freedom of expression. It is recommended that India follow the GDPR model where the data principal can directly contact the data fiduciary if he wishes to be forgotten.

***Include* Executive Agreements under the ambit Data Localization -** The Bill only requires sensitive personal data be mirrored within the territory of India. The Mutual Legal Assistance Treaties ('MLATs') signed between India and other countries are slow and inefficient in the retrieval of data of Indian citizens whose data may be stored in foreign servers. It is recommended that for the fast retrieval of data stored on foreign servers India should enter into executive agreements with countries which possess Indian data. The executive agreements will be alike the ones proposed by the United States of America ('US') under the Cloud Act and shall help in speedy and accurate retrieval of data.

***Remove*** the precondition that personal data must be shared to avail any service or benefit from the state. In Puttaswamy II, the Supreme Court expressed its unwillingness to allow the Government to expand the scope of 'subsidies, services and benefits' to widen the net of Aadhaar.[1] The Court further required that benefits and services as mentioned in section 7 of the Aadhaar Act have the color of subsidies, i.e. welfare schemes where Government intends to deliver benefits targeted at a particular deprived class. The Court also required that the expenditure for providing such subsidies be drawn from the Consolidated Fund of India.[2] The poor do not have any real choice or agency in deciding whether or not to share personal data with the state. This is because they are in desperate need to avail government welfare schemes. However, by making access to welfare schemes conditional upon compromising privacy, the provision may contravene the right to equality under Article 14 of the Constitution; in *effect*, the provision disproportionately restricts the right to privacy of the poor, who exercise no real choice in availing welfare benefits from the state. This makes the right to privacy illusory for the poor. The state should explore alternatives to making access to welfare conditional upon sharing personal data.

[1] K. S. Puttaswamy v. Union of India, (2018) 1 SCC 809, para. 322
[2] *Id.*

## II. SUMMARY OF STAKEHOLDER RECOMMENDATIONS

In an attempt to consolidate some of the concerns that have been voiced by major stakeholders in their respective comments on the current and previous versions of the Bill, this Report presents a documented list of broad recommendations made for the same.

1. The definition of financial data, as under Section 3(18) of the Bill, was seen to be restrictive in its scope and was recommended to include other financial information and not just numbers such as financial statements, financial transactions and use of financial services offered by the financial institutions.

2. The definition of genetic data under Section 3(19) of the Bill only consists of "*unique information about the behavioral characteristics, physiology or the health of that natural person*" which restricts the definition only to coding DNA. However, increasingly non-coding DNA, which does not give any information about physiology etc. but about genealogy and kinship, is being used for DNA profiling. DNA profiling is used to identify persons based on their kinship and genealogy. Thus, the definition of genetic data should be expanded to include the use and collection of such non-coding DNA.

3. The definition of 'harm' in Section 3(20) of the Bill further provides for a limited list of harms that do not account for new types of harm that may arise in the future owing to increased technological innovation. The list does not include harms such as psychological manipulation or impairing the autonomy of the person to make his/her own decisions by way of using artificial intelligence. Thus, the definition of harm needs to account for the flexibility to incorporate such future harms.

4. The definition of personal data in Section 3(28) of the Bill should also include identifiers which are meant to track the natural persons even if they are not combined with any characteristic, trait, attribute or any other feature of such a natural person. The Bill should also include a definition of '*identified*' and '*identifiable*' in line with the European Union's ('EU') Article 29 Working Party recommendation.[3]

5. The Bill should also be cognizant of the relationship of children with digital media in today's modern world and the age of maturity (and consent) should be accordingly reduced. The fiduciary should also have the responsibility of informing the children in a lucid manner how their data will be used.

6. The Bill provides no clear definition on what is '*clear*', '*specific*' and '*lawful*' under Section 4 of the Bill. The Data Protection Authority should have a responsibility to provide guidelines on what the standards of these terms should be. The terms '*reasonable*' and '*fair*' processing in Section 5 are seen as vague and broad terms which vests too much discretion to the data fiduciary. It is recommended that the Data Protection Authority formulates certain codes of

[3] "What is personal data?" European Commission, available at https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en (Last accessed on February 25th, 2020).

practice to delineate the contours of the same. The incidental purpose clause in Section 5(b) is very wide and should instead be replaced with the compatible purpose standard wherein the processing should be compatible with the purpose for which data had been collected initially.

7. Section 11 of the Bill envisages a blanket consent provision which is to be obtained at the time of commencement of processing. However, with the use of data becoming more pervasive, it is recommended that the consent should be obtained at each stage where the processing is carried out in a way for which the data subject had not consented to earlier.

8. Section 25 of the Bill stipulates that the data fiduciary is only liable to disclose information regarding a data breach which is likely to cause harm to any data principal. Thus, the discretion is very broad and problematic to determine the threshold of such harm. The discretion vested on the Data Protection Authority whether or not to make the data subject aware of such breach is also vague and discourages context-specific remedial actions as the Authority is ill-equipped to deal with the same. From an insurance perspective, such wide discretions leading to non-disclosure of breaches will make customers less aware of cyber risk and hence, likely to take cyber insurances.

9. The provisions for Data Localizations within the Bill adopt a '*one-size-fits-all*' approach. It is recommended that further analysis needs to be carried out to understand the relationship between international forces and domestic mandates so as to develop a context and sector specific framework for data localization. Section 33 of the Bill also provides that '*critical personal data'* shall not be processed anywhere apart from a server or a data centre located in India. The Central Government is tasked with notifying what shall constitute such critical personal data. The discretion granted to the Government in this regard is seen to be without sufficient guiding principles on how to determine the same.

10. Section 42 of the Bill stipulates that the Data Protection Authority should comprise of one Chairperson and six whole-time members. This provision does not provide for part-time or non-executive members. The appointment of non-executive members is seen to be desirable as they would function like unbiased members and bring a degree of objectivity in the functioning of the Authority. Various facets of the DPA's nature and functioning such as procedure to be adopted for the Selection Committee, remuneration of the members, meetings of the Authority have been left to the Central Government to form rules in that regard without any guidelines or framework based on which such regulations should be formulated.

# III. DETAILED COMMENTS

## *A. POWER TO NOTIFY CRITICAL PERSONAL DATA ONLY WITH CENTRE*

First, this results in over-centralization of power to regulate safeguards relating to public records inconsistent with the federal structure of the Constitution. Other laws regulating the flow of data distribute power to notify critical resources between the centre and the states. For instance, under section 70 of the Information Technology Act, 2000, the power to notify any computer resource (i.e. inter alia data) which affects critical information infrastructure as a 'protected system' vests with the 'appropriate government'.[4] The appropriate government is the State Government in relation to matters enumerated in List II and in respect of State laws enacted under List III of the Seventh Schedule of the Constitution. In respect of remaining matters, the Central Government has this power. Such a distinction remains absent in the Bill. Land records, for instance, involve public expenditure from the state consolidated fund and are in essence matters enumerated in the State list. Only the respective State governments should have the power to regulate or digitize land records, and other matters pertaining to List II.

It is suggested that the pith and substance of a law on data protection, in the context of a State is the right to regulate access to state records.[5] Therefore, in regulating data relating to records which fall within the domain of the state, such as state taxes, state services, land records, etc. the power should lie with the respective state. Similarly, with respect to records created by the Parliament, such as education records of central universities, employment records, income tax records, etc. the power to notify them as critical personal data should remain with the Parliament. The distribution of powers between the Centre and the State in notifying greater standards of protection/safeguards for critical data is not unprecedented; the Information Technology Act definition of appropriate government consciously acknowledges this distinction.

## *B. NO GUIDING EXPLANATION IN NOTIFYING CRITICAL PERSONAL DATA*

Second, there is no guiding principle that the Central Government is to follow in notifying categories of critical personal data. Under the Information Technology Act, however, Critical Information Infrastructure is defined to include "*computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety*". The absence of any guiding principle may result in excessive delegation of administrative powers. B.N Srikrishna, J in the decision of the Supreme Court in *Krishna Mohan Pvt. Ltd.* v. *Municipal Corporation of Delhi*[6] invalidated section 116(3) of the Delhi Municipal Corporation Act, 1957 for delegating unguided and un-canalized legislative powers to the Commissioner to declare any machinery or plant as part of the building or land to determine the rateable value of property tax.

---

[4] The Information Technology Act, 2000, §70.

[5] Prashant Reddy, Should States Have the Power to Enact their Own Data Protection Laws?, The Wire, December 22, 2017, available at https://thewire.in/tech/states-power-enact-data-protection-laws (Last accessed on February 25th, 2020).

[6] Krishna Mohan Pvt. Ltd. v. Municipal Corporation of Delhi, AIR 2003 SC 2935.

We recommend that the definition of critical information infrastructure be imported from the Information Technology Act, 2000 into the Bill. This would ensure that there are not adequate guiding principles in the Bill to preclude arbitrary notification of critical personal data.

### *C. ALGORITHMIC TRANSPARENCY AND EXPANDING THE RIGHT TO CONFIRMATION AND ACCESS*

At present, there is an increasing reliance on algorithms to achieve public policy goals.[7] Due to the proliferation in algorithmic decision-making, there must be a corresponding increase in government accountability for use of algorithms. This would help make the decision-making transparent and empower the data principal in making more informed decisions with respect to availing goods and services in the digital economy.

Under the Bill, there exists at present a right to access a summary of processing activities undertaken by the data fiduciary. This should be supported with a right to access the underlying logic or rationale behind the processing itself.

There exists an exemption under section 8 of the Right to Information Act, 2005 preventing an obligation to disclose trade secrets.[8] However, the need for algorithmic transparency can be reconciled with the need to protect trade secrets. One way in which this can be done is by creating a framework that requires data fiduciaries to undertake black box testing as a part of their privacy by design obligations.[9]

We recommend that the right to access be expanded to include the right to access the general controlling or guiding principles behind the decision-making. Data principals should be able to know the variables used in an algorithm to be able to investigate the existence of bias. This would only require the data fiduciary to share snippets of the algorithm or code or the training documentation used in programming the algorithm. Therefore, we suggest the following inclusion:

> *"17. (1) The data principal shall have the right to obtain from the data fiduciary— […] 17(1)(d) the general controlling principles guiding the processing of personal data."*

### *D. INDEPENDENCE OF CONSENT MANAGERS FROM THE DATA FIDUCIARY*

The Bill allows data principal to appoint consent managers who may consent on behalf of the data fiduciary. There are no conditions to regulate the appointment of a consent manager under the Bill. The consent manager can be any entity or individual, regardless of their relationship with the data fiduciary in question.

We feel that there is a need to regulate consent managers adequately by creating sufficient safeguards within the framework of the Bill. Stronger regulation of entities managing consent,

---

[7] United Nations Economic & Social Council of Asia Pacific, Artificial Intelligence in the Delivery of Public Services, October 16, 2019, available at https://www.unescap.org/publications/artificial-intelligence-delivery-public-services (Last accessed on February 25th, 2020).

[8] The Right to Information Act, 2005, §8.

[9] Ben Rashkovich, Government Accountability in the Age of Automation, April 9, 2019, available at https://law.yale.edu/mfia/case-disclosed/government-accountability-age-automation (Last accessed on February 25th, 2020).

particularly with respect to financial information providers is not unprecedented. The Reserve Bank of India regulates businesses which perform the function of consent management already vide its Master Direction 'Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016'.[10] These Directions were issued to 'Account Aggregators' for the purposes of regulatory compliance.

Account Aggregators are Non-Banking Financial Companies notified under section 45-I of the Reserve Bank of India Act, 1934[11]. In other words, account aggregators are consent brokers responsible for mediating transfer of data across different financial entities with the consent of users. Account aggregators enable structured sharing of financial data from financial information providers to financial information users. Account aggregators maintain a log of instances where consent is given, known as consent artifacts. Account aggregators allow individuals to revoke and manage consent. Entities in the financial sector which offer financial products and services are termed as financial information providers.

The Master Direction stipulates that account aggregators must register with the RBI.[12] It requires Account Aggregators to inter alia have an adequate capital infrastructure and robust information technology system. Account aggregators are precluded from engaging in businesses other than the business of account aggregation. Furthermore, account aggregators cannot deploy investible surplus into non-tradable instruments.

We envisage a situation where the data fiduciaries themselves may create consent managers (example, the data fiduciary's subsidiary entity). The data fiduciary and the consent manager could often be related parties who may engage in inter-se arrangements to share data. While these arrangements may involve the consent of the data principal, such consent may not be informed (since the consent manager is not obligated to disclose the relationship between the data fiduciary and the consent manager to the data fiduciary). This may lead to a situation where registered consent managers could take decisions on behalf of the data principal prejudicial to their interests. In a given situation, an entity or individual should not be permitted to become a consent manager if they are an entity directly or indirectly related to the data fiduciary processing the data of the data principal. However, at present there are no restrictions in the Bill precluding consent managers from processing the personal data of the data principal for its own interests. The consent manager could be engaged in several other businesses, or, corollary, other technology companies could themselves be engaged in the business of consent management. These situations would involve convergence of interests between the data fiduciary and the consent manage in a given case.

Convergence of interests or same interests (when the consent manager and the data fiduciary are for all practical purposes the same entity) may result in decision-making which is not in the best interests of the data principal.

---

[10] Master Direction 'Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016', available at https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598 (Last accessed on February 25th, 2020).

[11] The Reserve Bank of India Act, 1934.

[12] Master Direction 'Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016', available at https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598 (Last accessed on February 25th, 2020).

### *E. FIDUCIARY DUTIES*

The Bill defines entities which control the processing of personal data as data fiduciaries. However, existing obligations under the Bill may not require the data fiduciaries to undertake an adequately high standard of duty of loyalty and care, which form the essence of every fiduciary relationship. Courts in India require a very high standard of power differential in order to regard a relationship as 'fiduciary'.[13] In a series of decisions, Courts have held that relationships of service are not actually fiduciary in nature.[14] In every exchange of information, the relationship between parties is not necessarily one which is '*fiduciary*'.

We feel there is a need to include within the text of the Bill a general obligation to undertake the duty of loyalty. Data fiduciaries must not use personal data or information derived from personal data which benefits the data fiduciary in a manner which causes harm to the data principal in a manner which is reasonably foreseeable. Data processing entities should also be required to place the interests of the data principal ahead of their own to avoid conflict of interests.

This has in fact been attempted in the federal Data Care Act, 2019, a proposed legislation in the United States of America.[15] Notably, these laws specifically deem data processing entities as fiduciaries thereby requiring them to place their user's interests ahead of their own, and avoid acting in a manner that could be considered unexpected or offensive to a reasonable user. In this context, it is interesting to note the draft PDP Bill does in fact attempt to cover even "inferred" data within its ambit - i.e. information that is gleaned from analyzing personal information.

We believe that terminologically defining the relationship between the entity processing personal data and the data subject as 'fiduciary' may not be adequate for Courts to impose the high standards of duty of care, loyalty and confidentiality typical of a fiduciary relationship. Several proposed legislations, including New York's Privacy Act and the Federal Data Care Act impose fiduciary duties upon entities which process personal data. Fiduciary obligations operate irrespective of whether or not the data principal consents to processing. Therefore, we recommend the following draft provision to be added to Chapter II:

"*Data fiduciaries shall not use personal data or data derived from personal data when it is reasonably foreseeable that such use harms the data principal; and*

*Data fiduciaries may not transfer personal data to third parties unless it enters into a contract with third parties which imposes the same obligations towards the data principal, notwithstanding anything in this Act.*"

### *F. EXCLUDING ANONYMISED PERSONAL DATA FROM SECTION 91*

[13] Rishabh Bailey & Trishee Goyal, Fiduciary relationships as a means to protect privacy: Examining the use of the fiduciary concept in the draft Personal Data Protection Bill, 2019, The Leap Blog, January 13, 2020, https://blog.theleapjournal.org/2020/01/fiduciary-relationships-as-means-to.html (Last accessed on February 25th, 2020)

[14] *Id*; For a detailed explanation see Central Board of Secondary Education & Anr. v. Aditya Bandopadhyay, Civil Appeal No.6454 of 2011.

[15] The Data Care Act, 2019 (USA).

The Central Government through section 91 of the Bill can direct data fiduciaries to share anonymised personal data or other non-personal data. We feel that this provision should be removed since currently, there is no method of anonymisation which can result in re-identification in a manner which is reasonably impracticable.[16] Any standard of anonymisation notified by the DPA may therefore be inadequate to safeguard such personal data. A minimum standard of anonymisation only ensures a bare minimum degree of safeguard against re-identification of de-identified personal data. In the absence of a reliable standard of anonymisation at this juncture, we believe that enabling sharing of personal data in this manner would be against the reasonable expectation of privacy as laid down in Puttaswamy I. The right to privacy is exercised against both private parties and the state. We suggest the exclusion of anonymised personal data from the scope of this provision. This would protect against the risk of development of new methods of re-identification by development of technology (such as the use of brute force to re-identify, etc). The reasonable expectation of privacy continues to operate irrespective of whether or not the personal data has been anonymised. Anomysation per se does not enable absolute restriction on the fundamental right to privacy. Therefore, we recommend the following amendment to section 91:

> *"The Central Government may, in consultation with the Authority, direct any data fiduciary or data processor to provide any non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in such manner as may be prescribed*
>
> *Notwithstanding anything contained under this Act, anonymised personal data shall not be shared*
>
> *Explanation.—For the purposes of this sub-section, the expression "non-personal data" means the data other than personal data and excludes anonymised personal data."*

### *G. LIABILITY FOR JOINT CONTROLLERS MISSING: TAKING FROM THE TRUST ACT*

The Bill defines data fiduciaries to envisage entities which control processing over personal data in conjunction with one another, i.e. joint data fiduciaries. The Bill, however, does not stipulate which data fiduciary can the data principal/data protection authority proceed against when there is a breach of obligation by either party. When control over processing of personal data is exercised jointly by more than one data fiduciary, principles of apportioning liability could be borrowed from the existing framework of liability for co-trustees under the Trust Act. This ensures that the data principal has the liberty to proceed against any one of the joint data fiduciaries. Under the Trust Act, when co-trustees commit a breach of trust (similar to a breach of fiduciary obligations), or when the neglect by one trustee enables the other to commit a breach of obligations, each co-trustee is held liable for the whole of the loss occasioned by such breach. As between themselves, if one be less guilty than another and has had to refund the loss, the former may compel the latter, or his legal representative to the extent of the assets he has received, to make good such loss; and if all be equally guilty, any one or more of the trustees who has had to refund the loss may compel the others to contribute.

[16] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm (Last accessed on February 25th, 2020).

### *H. INDEMNITY CONTRACTS AGAINST PENALTIES FOR BREACHING OBLIGATIONS UNDER THE BILL MUST BE EXPRESSLY PRECLUDED*

For breach of obligations under section 57, there is only a corresponding sanction in the nature of a monetary compensation and no corresponding imprisonment prescribed under the Bill. The sanction of monetary compensation may often not be a sufficient disincentive for data fiduciaries from breaching these obligations. However, monetary costs may be indemnified if the data fiduciary enters into a contract of insurance with an insurance company. Data fiduciaries may engage in a cost-benefit analysis and realize that it is more beneficial to breach the obligation (in terms of benefit from the processing) compared to the compensation. This is because data fiduciaries can make enormous amounts of profit from big data analytics, etc. for which the compensation prescribed in the Bill may not be adequate. While Indian courts have not had the opportunity to examine whether contract law in India allows data fiduciaries to insure themselves against penalties from breach of obligations under the Bill. In India, contracts that are opposed to public policy are not enforceable. Indian Courts have not had an opportunity to examine the question of law as to whether a contract of indemnity exculpating responsibility for committing a data breach is a breach of public policy and therefore unenforceable. Encouraging cyber insurance against deliberate breach of obligations can encourage a moral hazard, i.e. data fiduciaries can priorities expenditure on indemnity arrangements as opposed to undertaking periodic checks over their security infrastructure and compliance with existing obligations under the Bill. We therefore recommend that the following provision be included into the text of the Bill:

> *"Notwithstanding any contained in any other law in force, data fiduciaries shall not enter into a contract to indemnify against penalties arising out of the breach of any obligations under this Bill."*

### *I. LEGACY DATA*

Data of the deceased can reveal important details about people that are living and thus it is important that privacy is maintained even after the death of the individual. Post-mortem privacy is vital so that an individual can control his/her personal information even after their death. This can be compared with the moral right that exists in copyright jurisprudence, even after the death of the individual. This moral right over the copyrighted work can be enforced by his/her legal representatives. However, it is unclear from the bill whether the duties of data fiduciaries established prior to death extends beyond death. The data fiduciary upon the death of a data principal should not have unlimited control of the personal data of the deceased.

The French Act, *Loi Pour Une République Numérique*, a GDPR compliant law, allows citizens to set general or specific directives for the preservation, deletion, and disclosure of their personal data after death. These directives are subsequently registered with the various data fiduciaries that have a hold of the data. Similarly, the Bill should allow for the same.

It is our suggestion that data fiduciaries shall in its agreement with the data principal, require the data principals to mention the representative who would have the ability to exercise control over further authorizing the processing of their personal data after their death. Such representative would be regarded as the legacy data principal. We recommend the insertion of the following provision:

"*The legacy data principal shall have the right to:*

*11. Withdraw consent to further process personal data as provided in section 11(2)(e).*

*12. Access the data of the deceased data principal unless expressly barred by the data principal.*

*13. Right to erasure under section 18.*

*Provided that in case of death of the data principal, the data shall only be used in an anonymized form*;

*Further, the data of the data principal shall become a part of the public record, 30 years from the date at which the data principal passed away. Notwithstanding anything in this provision, exceptions encapsulated within Section 12 will apply to the legacy data of the deceased."*

*J. SECTION 19*

Section 19(2) carves out certain exceptions and states that the right to data portability and the provisions of S.19(1) will not be applicable in certain cases. Section 19(2)(a) exempts this right when the processing of the data is necessary for functions of the state. The wording of the statute is vague and gives wide discretion to the government to disregard the element of consent. Therefore, it is suggested that the proportionality test in the Puttaswamy judgement should be incorporated in the provision. The rights of citizens should only be curtailed to the extent that is necessary and proportionate, thus broad provisions that exempt the government do not adhere to this principle.

"*Section 19(2). The provisions of sub-section (1) shall not apply where —*

*(a)for the performance of any function of the State authorized by law for—*

*(i) the provision of any service or benefit to the data principal from the State; or*

*(ii) the issuance of any certification, license or permit for any action or activity of the data principal by the State;*

*(b) under any law for the time being in force made by the Parliament or any State Legislature; or*

*(c) for compliance with any order or judgment of any Court or Tribunal in India;*

*(d) to respond to any medical emergency involving a threat to the life or a severe threat to the health of the data principal or any other individual;*

*(e) to undertake any measure to provide medical treatment or health services to any individual during an epidemic, outbreak of disease or any other threat to public health.*"

Alternatively, the provision could include:

"*Section 19(2) -The provisions of sub-section (1) shall not apply where—*

*for the performance of any function of the State authorized by a law made by parliament.*"

This ensures that there is no arbitrariness in determining what right overrides the right to data portability.

## *K. SURVEILLANCE*

### *a. Definition of Surveillance*

Surveillance and observation, when not reasonably expected, has been provided by the Bill as an actionable harm, it becomes imperative that such a term be defined so as to reduce the degree of vagueness contained in the said provision. By the inclusion of such definition, the data principal would be in a better position to predict the circumstances in which he/she may move against the data fiduciary, which in turn, will be better placed to address what may cause harm to the data principal.

The following provisions allow for state-sanctioned surveillance:

1. Section 5 of Indian Telegraph Act, 1885 empowers governments to take possession of licensed telegraphs and to order interception of messages.
2. Rule 419A under Section 5(2) of the Indian Telegraph Rules, 1951 provides the procedures governing telephone tapping.
3. Section 69 of the Information Technology Act, 2000 empowers Central or State Government or officers specially authorized by the Government to issue directions for interception or monitoring or decryption of any information through any computer resource.
4. Section 69B of the Information Technology Act, 2000 empowers the Central Government to authorize any agency of the Government to monitor and collect traffic data or information through any computer resource for cyber security.
5. Section 28 of the Information Technology Act, 2000 empowers the Controller of Certifying Authorities (CCA) or authorized officers to investigate contraventions of the Act, rules or regulations made thereunder. Further, Section 29 empowers CCA or authorized officers the power to access computers and their data, on a reasonable cause to suspect that contravention of the Act has taken place.
6. Rule 3(7) of the Information Technology (Intermediaries Guidelines) Rules, 2011 requires that intermediaries such as ISPs and on-line portals must provide information or any assistance to authorized government agencies for the purpose of identity verification, prevention or investigation of offences, etc.
7. Rule 7 of the Information Technology (Guidelines for Cyber Cafe) Rules, 2011 directs cyber cafe owners to provide every related document, register and necessary information to the inspecting officer authorized to check cyber cafes and computer resources or network established therein.

It is pertinent to note that none of the two legislations, or the rules published thereunder, have defined surveillance or observation. Thus, we recommend the following draft definition for the purposes highlighted above, which may be added to Section 3 of the Bill:

> *"Surveillance means the intentional acquisition or interception by an electronic, mechanical, human or other means of collecting information regarding a person or group of persons, as defined under this Act."*
>
> *"Observation means subjecting the data principal to the sensory perception of another person, as defined under this Act."*

*b. Procedure and Preconditions for The Grant of an Order for Surveillance*

Since the current surveillance regime is governed by pre-Puttaswamy legislations, such as the Information Technology Act and the Telegraph Act, there is a need to enact a protection framework imbibing the principles of right to privacy laid down by the Supreme Court. Further, the relevant factors to be considered may also include a comparative analysis of the practice across jurisdiction regarding the conditions within which the Government, or any agency authorized thereby, may conduct surveillance.

In 2017, the Supreme Court in *K.S. Puttaswamy* v. *Union of India*[17] ('Privacy Judgment') held while the fundamental right to privacy is subject to reasonable restrictions, the restrictions have to meet a three-fold requirement, namely: (i) existence of a law; (ii) legitimate state aim; (iii) proportionality.

To this effect, the Supreme Court in *K.S. Puttaswamy* v. *Union of India*[18] ('Aadhaar Judgement') noted that "*an executive notification does not satisfy the requirement of a valid law contemplated under Puttaswamy. A valid law in this case would mean a law passed by Parliament, which is just, fair and reasonable. Any encroachment upon the fundamental right cannot be sustained by an executive notification.*" Further, the Supreme Court read down the 'national security' exception which provided access to the biometric database to the investigative agencies on authorization by the Joint Secretary. In holding that the joint secretary – a bureaucrat under the government of the day – is not the proper authority to decide whether such access should be given, the Court hinted that instead a judicial officer should be consulted.

Finally, it is pertinent to note that the decision of the Supreme Court in *People's Union for Civil Liberties* v. *Union of India*[19] failed to recognize a requirement of judicial oversight considering the fact that there was an absence in Indian law permitting judicial oversight of surveillance orders and also the fact that in the parallel United Kingdom law, the 'Interception of the Communications Act, 1985,' interception did not require judicial oversight. Following the judgment, the guidelines were codified in Rule 419(A) of the Indian Telegraph Rules, 1951 in 2007. As per Rule 419(A), a direction for interception under Section 5(2) may be issued only by the Union Home Secretary at the Centre, or the State Home Secretary or in unavoidable circumstances, by another authorized officer.

[17] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[18] K.S. Puttaswamy v. Union of India, (2019) 1 SCC 1.
[19] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.

However, global developments changed its course in the years following the judgement. The same resulted in the United Nations General Assembly Resolution on 'Privacy in the Digital Age' as well as the UN Human Rights Council's International Principles on the Application of Human Rights to Communication Surveillance. Both these principles emphasize the need for an independent authority responsible for granting the power to surveil in order to ensure greater accountability and independence. While the same was reiterated by the European Court of Human Rights, even the United Kingdom legislation that was previously relied upon was repealed and replaced by the Investigatory Powers Act, 2016, which mandated the approval of all warrants to surveil by independently appointed Judicial Commissioners and also sets up an Investigatory Powers Tribunal for all appeal purposes.

In light of these global developments, we recommend that the Data Protection Act, 2019 be the instrument to supplant adequate safeguards to the previous legislations in providing both judicial oversight - in terms of approval of the warrants issued by the Central/State government - and confer to the Appellate Tribunal the expanded jurisdiction to hear matters in this regard. Concurrently, the preconditions in order to grant the power to surveil must fall in line with the principles as laid down by the Supreme Court and an additional factor of an '*overriding state interest*' must be present in order to satisfy the reasonable abrogation of a fundamental right.

*c. Admissibility of Unconstitutionally Obtained Evidence*

One important consequence of the Privacy Judgment was that the evidence obtained *via* an unauthorized search, seizure or surveillance now came to be classified as unconstitutionally obtained evidence, rather than mere illegally obtained evidence. This distinction was drawn by the three-judge bench of the Supreme Court in *Selvi* v. *State of Karnataka*.[20] Here, the Court emphasized that while the latter nature of evidence would be inadmissible unless relevant, the former nature of evidence would be inadmissible in all circumstances. Thus, since the Puttaswamy Privacy judgment delegitimizes the obtaining of evidence when unauthorized by an Act of Parliament, and in the absence of circumstances exhibiting a proportionality and legitimate state aim, such evidence should be declared as inadmissible in a court of law. While this pronouncement has been accepted by a two-judge bench of the Bombay High Court,[21] the same may be codified in this Bill, since the intent and purpose of this act, as may be evidenced by the preambulatory phrases "*[...] to provide for protection of the privacy of individuals relating to their personal data [...]*" and "*[...] remedies for unauthorized and harmful processing [...]*", is to safeguard the interests of the data principal.

*d. Rights of Data Principals Subject To Surveillance*

While the Indian Telegraph Act and the Information Technology Act impose a penalty on the unlawful and unauthorized interception or acquisition of information that is protected by the right to privacy, neither legislation provides for a right to challenge the order sanctioning such surveillance. Since the order provided for under these legislations are executive in nature, they are not free from judicial scrutiny and oversight.

[20] Selvi v. State of Karnataka, (2010) 7 SCC 263.
[21] Vinit Kumar v. Central Bureau of Investigation, Economic Offences Department, W.P. No. 2637 (2019).

It is our recommendation that the data principal be provided the right to challenge the surveillance order after due notice of the same has been given to the data principal. For this purpose, the Bill should also enumerate reliefs that may be sought in this regard. As suggested above, these challenges may lie to an Appellate Tribunal established by the Bill itself.

## *L. WITHDRAWAL OF CONSENT*

### *e. Requirement of a Valid Reason*

Under Section 11(6) of the Bill, a data principal is required to produce a valid reason for the purpose of withdrawing consent from the processing of his/her personal data in order for no legal consequences to follow from such action.

There is a need to clarify why such a requirement exists. Indeed, as indicated by Section 11(2)(e), the ease with which withdrawal of consent may be executed should be comparable to the ease with which the consent was given in the first instance. Further, there is no indication within the Bill as to the factors relevant for adjudging validity of a reason given, or which authority, executive or judicial, shall be making such a determination.

It is our suggestion that this clause be removed from the Bill as earlier provisions, such as Section 4 and Section 7(1)(d), specify that the data fiduciary is required to first receive the consent of the data principal for the processing of the latter's personal data and that the latter possesses a right to withdraw his/her consent from the same. A similar provision is also contained under Section 5(7) of the Information Technology Rules, 2011 and Section 7(3) of the General Data Protection Regulation.

### *f. Consequences of Withdrawal of Consent*

While Section 11(6) of the Bill provides for an attribution of legal consequences arising out of the withdrawal of consent from the processing of data by the data principal, it is yet unclear what such legal consequences may be.

It is our suggestion that a specific clause be added to Section 7(1) requiring data fiduciaries to enlist consequences of the withdrawal of consent, if any. The same may also be added within the provisions for the publication of a privacy by design policy as provided for under Section 22 of the Bill. This would allow data principals to truly provide an informed consent as provided for by the *Puttaswamy* Judgment. The vagueness in this provision needs to be cured lest it deters the withdrawal of consent by data principal, rendering the obligation to obtain consent obsolete.

## *M. REGULATORY SANDBOXES*

### *g. Selection Criteria and Regulatory Regime*

A Regulatory Sandbox has been defined as a controlled/test regulatory environment for the live testing of new products or services in which regulators may (or may not) permit certain regulatory relaxations for the limited purpose of the testing. The Reserve Bank of India recently published the 'Enabling Framework for Regulatory Sandbox', providing for the functioning of a regulatory sandbox particularly in the Fintech (or Financial Technology) Sector. The Framework provides for a fixed selection process for those eligible to participate in the Sandbox, such as:

1. Incorporation and registration in India and compliance with DIPP Notification No. G.S.R. 364(E) dated April 11, 2018;

2. A minimum net worth of Rs. 50 lakhs;

3. A satisfactory CIBIL or equivalent credit score of the promoter(s)/director(s)/ entity;

4. Provisions for adequate safeguards built in its IT systems to ensure that it is protected against unauthorized access, alteration, destruction, disclosure or dissemination of records and data; among others.

These specifications allow for the protection of consumers by ensuring that the participants are in a position to bear any liability arising out of the experimental activities, while also granting customers a minimum degree of security. The Bill, however, allows all those participants whose 'Privacy by Design' policies have been approved by the Data Protection Authority. Such wide leverage lacks the additional degree of safeguards that necessarily needs to be employed by participants in order to allow them to function within a reduced regulatory regime. Therefore, it is not clear why the Sandbox regime within the Bill departs from that which was established by the Reserve Bank of India. The latter has also undergone rounds of consultations by major stakeholders and thus, is under review for upgrade. Thus, our suggestion is to align the requirements for participation under the two regimes as the latter contains a higher degree of safeguards than the former. The same may be formulated as a set of guidelines prescribed to the Data Protection Authority.

*h. Deletion of Data Upon Expiry of Sandbox Duration*

Section 40(4)(c)(iv) allows participants of the Sandbox to bypass requirements under Section 9 of the Bill to ensure that no data is retained beyond the period necessary to satisfy the purpose for which it was processed. The period required for the purpose of testing out the new products or services would naturally be envisaged within the period for which the data fiduciary will be allowed to operate within the Sandbox. Post the completion of such a period, the participant is obligated to ensure compliance with the original regulatory requirements, including, say for example, those contained within Section 9 of the Bill. Hence, there seems to be a contradiction in allowing for the retention of data provided by the data principal after the expiry of the duration of the Sandbox. This should not be permissible as such data was collected while operating under relaxed regulatory guidelines, as provided for by Section 40(4) of the Bill. Not only does this allow for Sandboxes to act as a means to circumvent regulations, it would also go against the principles of consumer protection and fair competition.

## *N. FAILURE TO PROVIDE A REASONABLE EXPLANATION UNDER SECTION 58*

Under Section 58 of the Bill, the data fiduciary is required to provide a 'reasonable explanation' in order to justify non-compliance with its obligations under Chapter V, such as complying with the right to correction or erasure of the data principal. However, the phrase 'reasonable explanation' is ambiguous and not indicative of any principle or reasoning that the courts shall weigh the explanation against. It is our suggestion that an explanation be added which may read as:

> *"For the purposes of this section, reasonable explanation provided by the data fiduciary must be in furtherance of the fundamental right to freedom of speech and expression."*

This definition would be helpful in safeguarding data fiduciaries (such as Twitter) for instance, from being forced to delete existing information shared by third parties, which affects their right to disseminate or access such information. Take for instance, a re-tweet of an original tweet which invited public criticism. Even though the data principal from whom the tweet originated may want to delete their own tweet or post. The requirement that the reasonable explanation be in furtherance of freedom of speech limits the scope of explanation the data fiduciary may provide in precluding the data principal from exercising their right to be forgotten.

### *O. CONSULTATION V. CONCURRENCE UNDER SECTION 15*

The Central Government shall, in consultation with the Authority and the sectoral regulator concerned, notify such categories of personal data as "sensitive personal data", having regard to—

In this Section the word 'Authority' connotes the 'Data Protection Authority'. The word 'consultation' here implies that the Central Government shall take the view of the DPAs into account. The case, *Supreme Court Advocate-on-Record Association* v. *Union of India*[22] has held that 'consultation' is equivalent to 'concurrence', this has additionally been reiterated by the Supreme Court in the case *N. Kannadasan* v. *Ajoy Khose*.[23] The former case also held that "concurrence" was integral to maintaining an independent judiciary, and therefore is an essential feature of the Constitution. But subsequent cases such as *State of Rajasthan* v. *Harish Chandra*,[24] *Pruthvisinh Amarsinh Chauhan* v. *K.D. Rawat or His Successor in Office Secretary*[25] and *Dr. Cosmos John* v. *State of Bihar*[26] have held in various circumstances that consultation does not imply concurrence.

In this context to erase future concerns or confusion, the word 'consultation' in Section 15 be changed to 'concurrence'. The Data Protection Authority as stated under Section 42(2) of the Bill, are being appointed by the Central Government on the recommendation made by a selection committee. Section 42(4) further states that the DPA's members shall be "*persons of ability, integrity and standing, and shall have qualification and specialized knowledge and experience of, and not less than ten years in the field of data protection, information technology, data management, data science, data security, cyber and internet laws, public administration, national security or related subjects.*"

For the DPA to be functional and independent, it must be given complete autonomy. This autonomy must extend beyond judicial decisions for the DPA to be a meaningful and functional unit. In this regard the process of notifying categories of personal data as 'sensitive personal data' should be with the endorsement of the DPA. In the absence of such a provision the body will be bereft of any meaningful authority.

---

[22] Supreme Court Advocates on Record Association v. Union of India, AIR 1994 SC 268.
[23] N. Kannadasan v. Ajoy Khose, MANU/SC/0926/2009.
[24] State of Rajasthan v. Harish Chandra Sharma, RLW 2006 (4) Raj 3028.
[25] Pruthvisinh Amarsinh Chauhan v. K.D. Rawat or His Successor in Office Secretary, 2004 (2) GLH 640.
[26] Dr. Cosmos John v. State of Bihar & Ors, 2003 (3) BLJR 1734.

The Central Government under Section 33 of the Bill has the separate power to notify what 'critical personal data' and therefore its powers remain unhindered. Moreover, Section 34(2) further allows the government to transfer critical personal data outside India as well. Therefore, the Government is not denied its powers by such a change.

### *P. RIGHT TO BE FORGOTTEN*

Section 20(2) of The Personal Data Protection Bill, 2019 requires that the rights to be forgotten may only be enforced on an order of the Adjudicating Officer made on an application filed by the data principal. The proviso under Section 20 further stipulates that no such order shall be made by the Adjudicating Officer unless the data principal shows that his right or interest in preventing or restricting the continued disclosure of his personal data overrides the right to freedom and expression and the right to information of any other citizen.

Section 62 of the bill further provides for the appointments of Adjudicating Officers. The Central Government under Section 62(2) has the authority to prescribe the number of Adjudicating Officers, manners and terms of appointment of the Adjudicating Officer and their respective jurisdiction. Essentially the Adjudicating officers are quasi-judicial but have been given the authority to choose what should and should not be forgotten.

There remains the potential for significant harm in handing over such power to the Officers. The remuneration, appointment and service conditions are all governed by the Central Government. Thus in effect, it is the Central Government which shall hold the power to decide what should be deleted.

As the comments from the Centre of Internet Society states, this clause has put a heavy burden on the authority who might not have the capacity to handle the flow of requests coming in. The Authority will additionally have to coordinate with the data fiduciary for each request making the process severely time consuming. This becomes especially pertinent in respect to personal data and sensitive personal data. Further, the need to provide an immaculate reason to the Adjudicating Officer hinders the pace of the process which may often require haste.

It is recommended that India follow the GDPR model. Article 17 of the GDPR (Right to be forgotten) states that there should be direct communication between the controller (in the context of India known as 'data fiduciary') and the data principal. If the Data principal seeks to exercise the right, he should directly be able to communicate such a request to the Data Fiduciary. This removes the DPA as an intermediary reducing the opportunity cost involved in the process. Furthermore, the data principal should not have to give the Data Officer such evidence to erase his personal data as provided in the proviso of Section 20. Even if merely one of the conditions is fulfilled under Section 20(1) it should suffice for the data principal to have his data erased.

### *Q. THE DATA LOCALIZATION CONUNDRUMS WITHIN THE PURVIEW OF INDIA*

The 2018 draft bill proposed that all data be localized within India but this was not considered feasible and was subsequently dropped. The 2019 Bill on the other hand only requires that sensitive personal data when being transferred out of India be mirrored within the territory of India. This, however, does little to solve the problem of the slow retrieval of data stored in foreign data servers. India is signatory to a number of MLATs which follow a certain process for data retrieval. Through this process, server providers can share metadata on request of foreign governments, but require a

judicially issued warrant based on a finding of 'probable cause' for a service provider to share content data.[27]

The challenges associated with accessing data across borders has been an area of concern for India for many years. From data localization requirements, legal decryption mandates, proposed back doors- law enforcement and the government have consistently been trying to find efficient ways to access cross-border data.[28]

Further the localization mandate for exclusively sensitive personal data extends only to Indian citizens. It does not solve, for instance, the issue that arose in the Microsoft-Ireland Case. In this case, the law enforcement agencies required access to data relating to a foreigner in a server located in another jurisdiction where the company itself was incorporated within the US.

One solution to this, also highlighted by the comments by the Centre of Internet and Society, is to follow the US model of data extraction from foreign servers as specified by the Clarifying Lawful Overseas Use of Data Act ('Cloud Act'). This law enables US law enforcement agencies to access data stored abroad.[29] Under this model, India can pursue executive agreements with countries which possess Indian data stored on their servers. These agreements will give the Indian government the power to enter into bilateral agreements with other countries that have adequate standards to ensure the safeguarding privacy, human rights and due process. MLATs require acceptance by the judicial authorities for the retrieval of data for both provider and receiver. These strict and time-consuming regulations can be bypassed through Ex

Another possibility is for India to follow the European Union Model. The European Commission proposed draft legislation on e-Evidence (both a Regulation and Directive) in April 2018 to facilitate cross-border data-sharing in the case of criminal investigations. As per the legislation, law enforcement authorities across EU member states can compel "production orders" from communication and cloud-based service providers inside or outside the EU regardless of where the data is located. The Directive further requires EU member states to establish legal representatives for the receipt of cross-border demands. Taken together, the Regulation and Directive would effectively give EU member states access for law enforcement purposes to the data of internet users not only across the EU, but worldwide. The EU's e-Evidence proposal, importantly, focuses on access, not location, and provides another potential model for addressing the law enforcement access problem in India.

Further, to be a part of the Cloud Act; Executive Agreements, the safe harbor principle needs to be applicable in the context of India. This would require India to rework its surveillance framework, bringing them in line with international standards of protection.

---

[27] Electronic Privacy Information Centre. Electronic Communications Privacy Act (ECPA). https://epic.org/privacy/ecpa/ (Last accessed on February 25th, 2020).

[28] Techdirt (2015, September 21). India's Government Looking At Mandating Backdoors In Encryption. https://www.techdirt.com/articles/20150921/07085332311/indias-government-lookingmandating-backdoors-encryption.shtml (Last accessed on February 25th, 2020).

[29] 18 U.S. Code §2513 - Confiscation of wire, oral, or electronic communication intercepting devices.

# IV. VISION FOR THE FUTURE: INCREASING DIGITAL LITERACY INITIATIVES

The Justice Srikrishna Committee Report had outlined a vision for data protection which emphasizes a '*free and fair digital economy*'. The report also discussed extensively about how a robust data protection framework is crucial in bringing forth the digital revolution, wherein India may shape the global digital landscape for the future. It is therefore important to note that while the committee suggested several ideas regarding the use of data in a transformative sense, its report and proposed bill submitted had little originality in terms of approach. In taking stock of international best practices, it creates a draft bill which lays the foundation for a digital India by aligning itself to these global standards. The report acknowledges the differing approaches adopted across jurisdictions and settles for a roughly–GDPR compliant model.

Critically, however, the report and subsequent bill fails in creating *an indigenous understanding of privacy* for India. Such an understanding is crucial for two reasons.

**Firstly, the indigenous, culture-specific needs of the Indian population may vary greatly from those of the Western nations, which have purportedly served as a model for the proposed framework. For instance, while established notions of informed consent have been incorporated in the draft bill, we believe such a conception to be insufficient in the Indian context.**

The issue of free and informed consent is central to protecting individual privacy and data protection. This has been stressed in several provisions of the current bill, which identifies individuals as the data principals and includes an express requirement of consent for collection and processing of their data.[30] Both the bills (2018 and 2019), however, do not so much as mention the issue of digital literacy. In India, where basic literacy is relatively low as compared to the developed countries - digital literacy is abysmal. This is evident from the burgeoning number of cyber-crimes reported every year, where commoners are swindled of their hard-earned money by fraudsters masquerading as bank employees and the like. Similarly, the massive proliferation of fake news and its impact on democratic processes within the country is an indicator of the power of social media platforms in manipulating minds. In this backdrop, it is clear that consent provides a necessary yet insufficient framework in protecting digital rights in India.

This inability in appreciating consent stems from the impossibility of explaining basic physical privacy to the regular Indian person. This becomes amply clear if we take the example of the lack of physical space within Indian homes. A third of urban houses in India are around 250 sq. ft. or lesser in size, and this figure goes up to about 310 sq. ft. for rural areas.[31] In other words, the per capita space in urban India is about 60 sq. ft., and about 65 sq. ft. in rural homes, for an average household of 4 persons. This is roughly the same size as a US prisoner occupies inside a jail cell.[32] Thus, for those to whom physical privacy is elusive, any attempt to explain the importance of

[30] The Personal Data Protection Bill, 2018, §12; The Personal Data Protection Bill, 2019, §11.
[31] Atul Thakur, 33% Indians live in less space than US Prisoners, The Times of India, November 25, 2008 available at https://timesofindia.indiatimes.com/india/33-of-Indians-live-in-less-space-than-US-prisoners/articleshow/3753189.cms (Last accessed on February 25th, 2020).
[32] *Id*.

abstract derivatives of this concept – such as data privacy – and the risks associated, is an exercise in futility.

It is our belief that in order for this vision of a digital India to materialize, there needs to be concerted efforts to educate our teeming millions about the necessity, importance and utility of using technology, as well as their rights and duties in the digital universe. The task is daunting for certain, but one that is absolutely critical to the ultimate success of such a venture. We propose a two-fold strategy in this regard. In the short-term, we propose the strengthening of the 'obligation to inform' that data principal of the manner of collection, use and analysis of the data to be collected, and such information being made available in the local language. For instance, the simplification of the software licensing agreements for mobile applications into a simple bullet-point format covering all essentials relating to the data, available in Hindi and other languages should be made mandatory. In the long-term, we find no alternative but for the government to begin awareness and mass education drives which spread the information about the rights of citizens under the digitization initiatives. This could be supplemented by advertisements and regular announcements, demonstrations on television etc., akin to the successful polio-eradication campaign, which would bring this information to the masses.

**Secondly, the data protection law provides India with a unique opportunity at shaping the debate at a normative level, and establishing India as a thought leader in data privacy and digitalization, instead of being a mere bystander in the discussions around and development of key concepts in this arena.**

While there seems some consensus on the necessity of a quality data protection regime, it is often contended that the idea of privacy is itself a Western concept. This is not necessarily true. As some researchers have established, the roots of the Indian privacy jurisprudence can be traced back to the Vedic Period.[33] In fact, evidence of privacy concerns within the Islamic legal traditions can also be observed, as practiced during the Mughal Period.[34] Thus, there seems enough reason to believe that privacy has been a subject of legal policymaking within the Indian context, and not an alien (primarily Western) transposition.

The reason we feel there is a need for an indigenous construct for privacy is manifold. As mentioned above, our peculiar socio-economic positioning and historical context should not be ignored while drafting a law which is likely to have substantial impact on the future of our polity. From development of Artificial Intelligence to regulating Cryptocurrency, the application of the data protection regime will likely be widespread. It is therefore important that instead of primarily relying on foreign jurisprudence, we attempt to reframe the issue on our own terms. It is clear from the text of the bill that some of these concerns have indeed been considered by the Committee with seriousness- for example, data sovereignty concerns seem to stand out even though there is great adherence to international standards. In addition to these, the data protection mechanisms across the globe are all at a relatively nascent stage, and this offers a unique opportunity for India to create a truly original framework, which could serve as a template for other nations, as the GDPR has

[33] Bhairav Acharya and Ashna Ashesh, Locating Constructs of Privacy within Classical Hindu Law, CIS Whitepaper available at https://cis-india.org/internet-governance/blog/loading-constructs-of-privacy-within-classical-hindu-law (Last accessed on February 25th, 2020).

[34] Bhairav Acharya and Vidushi Marda, Identifying Aspects of Privacy in Islamic Law, CIS Whitepaper available at https://cis-india.org/internet-governance/blog/identifying-aspects-of-privacy-in-islamic-law (Last accessed on February 25th, 2020).

done. This proposal is by no means a call to ignore established global principles governing data, but a call to promote greater innovation in developing a normative framework, which allows India to become a thought-leader in the arena of digitalization and data governance.