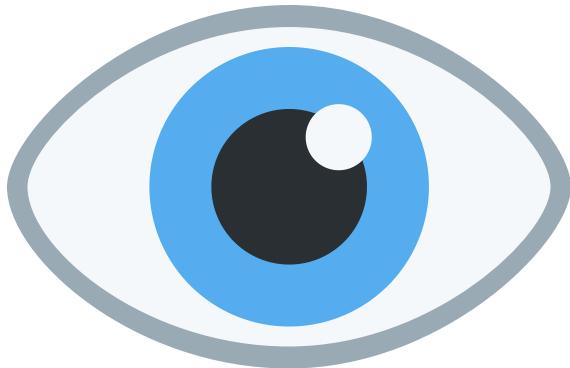


AN OVERVIEW OF THE BILL, ITS HISTORY,
CONCERNS, AND WHAT PEOPLE THINK ABOUT IT



A COMPLETE GUIDE TO THE PERSONAL DATA PROTECTION BILL

MEDIANAMA

TO BE INTRODUCED IN LOK SABHA

Bill No. 373 of 2019

THE PERSONAL DATA PROTECTION BILL, 2019

ARRANGEMENT OF CLAUSES

CLAUSES

CHAPTER I PRELIMINARY

1. Short title and commencement.
2. Application of Act to processing of personal data.
3. Definitions.

CHAPTER II

OBLIGATIONS OF DATA FIDUCIARY

4. Prohibition of processing of personal data.
5. Limitation on purpose of processing of personal data.
6. Limitation on collection of personal data.
7. Requirement of notice for collection or processing of personal data.
8. Quality of personal data processed.
9. Restriction on retention of personal data.
10. Accountability of data fiduciary.
11. Consent necessary for processing of personal data.

CHAPTER III

GROUNDS FOR PROCESSING OF PERSONAL DATA WITHOUT CONSENT

12. Grounds for processing of personal data without consent in certain cases.
13. Processing of personal data necessary for purposes related to employment, etc.
14. Processing of personal data for other reasonable purposes.
15. Categorisation of personal data as sensitive personal data.

CHAPTER IV

PERSONAL DATA AND SENSITIVE PERSONAL DATA OF CHILDREN

16. Processing of personal data and sensitive personal data of children.

CHAPTER V

RIGHTS OF DATA PRINCIPAL

17. Right to confirmation and access.
18. Right to correction and erasure.
19. Right to data portability.

(ii)

CLAUSES

20. Right to be forgotten.
21. General conditions for the exercise of rights in this Chapter.

CHAPTER VI

TRANSPARENCY AND ACCOUNTABILITY MEASURES

22. Privacy by design policy.
23. Transparency in processing of personal data.
24. Security safeguards.
25. Reporting of personal data breach.
26. Classification of data fiduciaries as significant data fiduciaries.
27. Data protection impact assessment.
28. Maintenance of records.
29. Audit of policies and conduct of processing, etc.
30. Data protection officer.
31. Processing by entities other than data fiduciaries.
32. Grievance redressal by data fiduciary.

CHAPTER VII

RESTRICTION ON TRANSFER OF PERSONAL DATA OUTSIDE INDIA

33. Prohibition of processing of sensitive personal data and critical personal data outside India.
34. Conditions for transfer of sensitive personal data and critical personal data.

CHAPTER VIII

EXEMPTIONS

35. Power of Central Government to exempt any agency of Government from application of the Act.
36. Exemption of certain provisions for certain processing of personal data.
37. Power of Central Government to exempt certain data processors.
38. Exemption for research, archiving or statistical purposes.
39. Exemption for manual processing by small entities.
40. Sandbox for encouraging innovation, etc.

CHAPTER IX

DATA PROTECTION AUTHORITY OF INDIA

41. Establishment of Authority.
42. Composition and qualifications for appointment of Members.
43. Terms and conditions of appointment.
44. Removal of Chairperson or other Members.
45. Powers of Chairperson.
46. Meetings of Authority.
47. Vacancies, etc., not to invalidate proceedings of Authority.
48. Officers and other employees of Authority.
49. Powers and functions of Authority.
50. Codes of practice.

CLAUSES

51. Power of Authority to issue directions.
52. Power of Authority to call for information.
53. Power of Authority to conduct inquiry.
54. Action to be taken by Authority pursuant to an inquiry.
55. Search and seizure.
56. Co-ordination between Authority and other regulators or authorities.

CHAPTER X

PENALTIES AND COMPENSATION

57. Penalties for contravening certain provisions of the Act.
58. Penalty for failure to comply with data principal requests under Chapter V.
59. Penalty for failure to furnish report, returns, information, etc.
60. Penalty for failure to comply with direction or order issued by Authority.
61. Penalty for contravention where no separate penalty has been provided.
62. Appointment of Adjudicating Officer.
63. Procedure for adjudication by Adjudicating Officer.
64. Compensation.
65. Compensation or penalties not to interfere with other punishment.
66. Recovery of amounts.

CHAPTER XI

APPELLATE TRIBUNAL

67. Establishment of Appellate Tribunal.
68. Qualifications, appointment, term, conditions of service of Members.
69. Vacancies.
70. Staff of Appellate Tribunal.
71. Distribution of business amongst Benches.
72. Appeals to Appellate Tribunal.
73. Procedure and powers of Appellate Tribunal.
74. Orders passed by Appellate Tribunal to be executable as a decree.
75. Appeal to Supreme Court.
76. Right to legal representation.
77. Civil court not to have jurisdiction.

CHAPTER XII

FINANCE, ACCOUNTS AND AUDIT

78. Grants by Central Government.
79. Data Protection Authority of India Funds.
80. Accounts and Audit.
81. Furnishing of returns, etc., to Central Government.

CHAPTER XIII

OFFENCES

82. Re-identification and processing of de-identified personal data.
83. Offences to be cognizable and non-bailable.

CLAUSES

84. Offences by companies.
85. Offences by State.

CHAPTER XIV

MISCELLANEOUS

86. Power of Central Government to issue directions.
87. Members, etc., to be public servants.
88. Protection of action taken in good faith.
89. Exemption from tax on income.
90. Delegation.
91. Act to promote framing of policies for digital economy, etc.
92. Bar on processing certain forms of biometric data.
93. Power to make rules.
94. Power to make regulations.
95. Rules and regulations to be laid before Parliament.
96. Overriding effect of this Act.
97. Power to remove difficulties.
98. Amendment of Act 21 of 2000.

THE SCHEDULE.

TO BE INTRODUCED IN LOK SABHA

Bill No. 373 of 2019

THE PERSONAL DATA PROTECTION BILL, 2019

A

BILL

to provide for protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the rights of individuals whose personal data are processed, to create a framework for organisational and technical measures in processing of data, laying down norms for social media intermediary, cross-border transfer, accountability of entities processing personal data, remedies for unauthorised and harmful processing, and to establish a Data Protection Authority of India for the said purposes and for matters connected therewith or incidental thereto.

WHEREAS the right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of informational privacy;

AND WHEREAS the growth of the digital economy has expanded the use of data as a critical means of communication between persons;

AND WHEREAS it is necessary to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress and innovation through digital governance and inclusion and for matters connected therewith or incidental thereto.

Be it enacted by Parliament in the Seventieth Year of the Republic of India as follows:—

CHAPTER I

PRELIMINARY

Short title and commencement.	1. (1) This Act may be called the Personal Data Protection Act, 2019.	
	(2) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint; and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the coming into force of that provision.	5
Application of Act to processing of personal data.	2. The provisions of this Act,—	
	(A) shall apply to—	10
	(a) the processing of personal data where such data has been collected, disclosed, shared or otherwise processed within the territory of India;	
	(b) the processing of personal data by the State, any Indian company, any citizen of India or any person or body of persons incorporated or created under Indian law;	15
	(c) the processing of personal data by data fiduciaries or data processors not present within the territory of India, if such processing is—	
	(i) in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within the territory of India; or	20
	(ii) in connection with any activity which involves profiling of data principals within the territory of India.	
	(B) shall not apply to the processing of anonymised data, other than the anonymised data referred to in section 91.	
Definitions.	3. In this Act, unless the context otherwise requires,—	25
	(1) "Adjudicating Officer" means the Adjudicating Officer appointed as such under sub-section (1) of section 62;	
	(2) "anonymisation" in relation to personal data, means such irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the Authority;	30
	(3) "anonymised data" means data which has undergone the process of anonymisation;	
	(4) "Appellate Tribunal" means the Tribunal established under sub-section (1) or notified under sub-section (4) of section 67;	
	(5) "Authority" means the Data Protection Authority of India established under sub-section (1) of section 41;	35
	(6) "automated means" means any equipment capable of operating automatically in response to instructions given for the purpose of processing data;	
	(7) "biometric data" means facial images, fingerprints, iris scans, or any other similar personal data resulting from measurements or technical processing operations	40

carried out on physical, physiological, or behavioural characteristics of a data principal, which allow or confirm the unique identification of that natural person;

(8) "child" means a person who has not completed eighteen years of age;

5 (9) "code of practice" means a code of practice issued by the Authority under section 50;

(10) "consent" means the consent referred to in section 11;

(11) "data" includes a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means;

10 (12) "data auditor" means an independent data auditor referred to in section 29;

(13) "data fiduciary" means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data;

(14) "data principal" means the natural person to whom the personal data relates;

15 (15) "data processor" means any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary;

20 (16) "de-identification" means the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal;

53 of 2005. (17) "disaster" shall have the same meaning as assigned to it in clause (d) of section 2 of the Disaster Management Act, 2005;

25 (18) "financial data" means any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal or any personal data regarding the relationship between a financial institution and a data principal including financial status and credit history;

30 (19) "genetic data" means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the behavioural characteristics, physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(20) "harm" includes—

(i) bodily or mental injury;

35 (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;

40 (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;

45 (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

<p>(x) any observation or surveillance that is not reasonably expected by the data principal;</p> <p>(21) "health data" means the data related to the state of physical or mental health of the data principal and includes records regarding the past, present or future state of the health of such data principal, data collected in the course of registration for, or provision of health services, data associating the data principal to the provision of specific health services;</p> <p>(22) "intra-group schemes" means the schemes approved by the Authority under clause (a) of sub-section (I) of section 34;</p> <p>(23) "in writing" includes any communication in electronic format as defined in clause (r) of sub-section (1) of section 2 of the Information Technology Act, 2000;</p> <p>(24) "journalistic purpose" means any activity intended towards the dissemination through print, electronic or any other media of factual reports, analysis, opinions, views or documentaries regarding—</p> <p style="margin-left: 2em;">(i) news, recent or current events; or</p> <p style="margin-left: 2em;">(ii) any other information which the data fiduciary believes the public, or any significantly discernible class of the public, to have an interest in;</p> <p>(25) "notification" means a notification published in the Official Gazette and the expression "notify" shall be construed accordingly;</p> <p>(26) "official identifier" means any number, code, or other identifier, assigned to a data principal under a law made by Parliament or any State Legislature which may be used for the purpose of verifying the identity of a data principal;</p> <p>(27) "person" includes—</p> <p style="margin-left: 2em;">(i) an individual,</p> <p style="margin-left: 2em;">(ii) a Hindu undivided family,</p> <p style="margin-left: 2em;">(iii) a company,</p> <p style="margin-left: 2em;">(iv) a firm,</p> <p style="margin-left: 2em;">(v) an association of persons or a body of individuals, whether incorporated or not,</p> <p style="margin-left: 2em;">(vi) the State, and</p> <p style="margin-left: 2em;">(vii) every artificial juridical person, not falling within any of the preceding sub-clauses;</p> <p>(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;</p> <p>(29) "personal data breach" means any unauthorised or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to, personal data that compromises the confidentiality, integrity or availability of personal data to a data principal;</p> <p>(30) "prescribed" means prescribed by rules made under this Act;</p> <p>(31) "processing" in relation to personal data, means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;</p>	<p>5</p> <p>10</p> <p>15</p> <p>20</p> <p>25</p> <p>30</p> <p>35</p> <p>40</p> <p>45</p>
21 of 2000.	

(32) "profiling" means any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interests of a data principal;

(33) "regulations" means the regulations made by the Authority under this Act;

5 (34) "re-identification" means the process by which a data fiduciary or data processor may reverse a process of de-identification;

(35) "Schedule" means the Schedule appended to this Act;

(36) "sensitive personal data" means such personal data, which may, reveal, be related to, or constitute—

(i) financial data;

10 (ii) health data;

(iii) official identifier;

(iv) sex life;

(v) sexual orientation;

(vi) biometric data;

15 (vii) genetic data;

(viii) transgender status;

(ix) intersex status;

(x) caste or tribe;

(xi) religious or political belief or affiliation; or

20 (xii) any other data categorised as sensitive personal data under section 15.

Explanation.— For the purposes of this clause, the expressions,—

(a) "intersex status" means the condition of a data principal who is—

(i) a combination of female or male;

(ii) neither wholly female nor wholly male; or

25 (iii) neither female nor male;

(b) "transgender status" means the condition of a data principal whose sense of gender does not match with the gender assigned to that data principal at birth, whether or not they have undergone sex reassignment surgery, hormone therapy, laser therapy, or any other similar medical procedure;

30 (37) "significant data fiduciary" means a data fiduciary classified as such under sub-section (I) of section 26;

(38) "significant harm" means harm that has an aggravated effect having regard to the nature of the personal data being processed, the impact, continuity, persistence or irreversibility of the harm;

40 (39) "State" means the State as defined under article 12 of the Constitution;

(40) "systematic activity" means any structured or organised activity that involves an element of planning, method, continuity or persistence.

CHAPTER II

OBLIGATIONS OF DATA FIDUCIARY

Prohibition of processing of personal data.

4. No personal data shall be processed by any person, except for any specific, clear and lawful purpose.

Limitation on purpose of processing of personal data.

5. Every person processing personal data of a data principal shall process such personal data—

(a) in a fair and reasonable manner and ensure the privacy of the data principal; and

(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.

Limitation on collection of personal data.

6. The personal data shall be collected only to the extent that is necessary for the purposes of processing of such personal data.

Requirement of notice for collection or processing of personal data.

7. (1) Every data fiduciary shall give to the data principal a notice, at the time of collection of the personal data, or if the data is not collected from the data principal, as soon as reasonably practicable, containing the following information, namely:—

(a) the purposes for which the personal data is to be processed;

(b) the nature and categories of personal data being collected;

(c) the identity and contact details of the data fiduciary and the contact details of the data protection officer, if applicable;

(d) the right of the data principal to withdraw his consent, and the procedure for such withdrawal, if the personal data is intended to be processed on the basis of consent;

(e) the basis for such processing, and the consequences of the failure to provide such personal data, if the processing of the personal data is based on the grounds specified in sections 12 to 14;

(f) the source of such collection, if the personal data is not collected from the data principal;

(g) the individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared, if applicable;

(h) information regarding any cross-border transfer of the personal data that the data fiduciary intends to carry out, if applicable;

(i) the period for which the personal data shall be retained in terms of section 9 or where such period is not known, the criteria for determining such period;

(j) the existence of and procedure for the exercise of rights mentioned in Chapter V and any related contact details for the same;

(k) the procedure for grievance redressal under section 32;

(l) the existence of a right to file complaints to the Authority;

(m) where applicable, any rating in the form of a data trust score that may be assigned to the data fiduciary under sub-section (5) of section 29; and

(n) any other information as may be specified by the regulations.

(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.

5 (3) The provisions of sub-section (1) shall not apply where such notice substantially prejudices the purpose of processing of personal data under section 12.

8. (1) The data fiduciary shall take necessary steps to ensure that the personal data processed is complete, accurate, not misleading and updated, having regard to the purpose for which it is processed.

10 (2) While taking any steps under sub-section (1), the data fiduciary shall have regard to whether the personal data—

(a) is likely to be used to make a decision about the data principal;

(b) is likely to be disclosed to other individuals or entities including other data fiduciaries or processors; or

10 (c) is kept in a form that distinguishes personal data based on facts from personal data based on opinions or personal assessments.

(3) Where personal data is disclosed to any other individual or entity, including other data fiduciary or processor, and the data fiduciary finds that such data does not comply with the requirement of sub-section (1), the data fiduciary shall take reasonable steps to notify such individual or entity of this fact.

15 **9. (1)** The data fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of the processing.

20 (2) Notwithstanding anything contained in sub-section (1), the personal data may be retained for a longer period if explicitly consented to by the data principal, or necessary to comply with any obligation under any law for the time being in force.

(3) The data fiduciary shall undertake periodic review to determine whether it is necessary to retain the personal data in its possession.

25 (4) Where it is not necessary for personal data to be retained by the data fiduciary under sub-section (1) or sub-section (2), then, such personal data shall be deleted in such manner as may be specified by regulations.

10. The data fiduciary shall be responsible for complying with the provisions of this Act in respect of any processing undertaken by it or on its behalf.

11. (1) The personal data shall not be processed, except on the consent given by the data principal at the commencement of its processing.

30 (2) The consent of the data principal shall not be valid, unless such consent is—

(a) free, having regard to whether it complies with the standard specified under section 14 of the Indian Contract Act, 1872;

(b) informed, having regard to whether the data principal has been provided with the information required under section 7;

35 (c) specific, having regard to whether the data principal can determine the scope of consent in respect of the purpose of processing;

(d) clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given context; and

40 (e) capable of being withdrawn, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given.

Quality of personal data processed.

Restriction on retention of personal data.

Accountability of data fiduciary.

Consent necessary for processing of personal data.

<p>(3) In addition to the provisions contained in sub-section (2), the consent of the data principal in respect of processing of any sensitive personal data shall be explicitly obtained—</p> <ul style="list-style-type: none"> (a) after informing him the purpose of, or operation in, processing which is likely to cause significant harm to the data principal; (b) in clear terms without recourse to inference from conduct in a context; and (c) after giving him the choice of separately consenting to the purposes of, operations in, the use of different categories of, sensitive personal data relevant to processing. <p>(4) The provision of any goods or services or the quality thereof, or the performance of any contract, or the enjoyment of any legal right or claim, shall not be made conditional on the consent to the processing of any personal data not necessary for that purpose.</p> <p>(5) The burden of proof that the consent has been given by the data principal for processing of the personal data under this section shall be on the data fiduciary.</p> <p>(6) Where the data principal withdraws his consent from the processing of any personal data without any valid reason, all legal consequences for the effects of such withdrawal shall be borne by such data principal.</p>	<p>5</p> <p>10</p> <p>15</p>
<h3>CHAPTER III</h3> <h4>GROUNDS FOR PROCESSING OF PERSONAL DATA WITHOUT CONSENT</h4>	
<p>12. Notwithstanding anything contained in section 11, the personal data may be processed if such processing is necessary,—</p>	<p>20</p>
<p>(a) for the performance of any function of the State authorised by law for—</p> <ul style="list-style-type: none"> (i) the provision of any service or benefit to the data principal from the State; or (ii) the issuance of any certification, licence or permit for any action or activity of the data principal by the State; <p>(b) under any law for the time being in force made by the Parliament or any State Legislature; or</p> <p>(c) for compliance with any order or judgment of any Court or Tribunal in India;</p> <p>(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;</p>	<p>25</p>
<p>(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; or</p> <p>(f) to undertake any measure to ensure safety of, or provide assistance or services to, any individual during any disaster or any breakdown of public order.</p>	<p>30</p> <p>35</p>
<p>13. (1) Notwithstanding anything contained in section 11 and subject to sub-section (2), any personal data, not being any sensitive personal data, may be processed, if such processing is necessary for—</p> <ul style="list-style-type: none"> (a) recruitment or termination of employment of a data principal by the data fiduciary; (b) provision of any service to, or benefit sought by, the data principal who is an employee of the data fiduciary; 	<p>40</p>

Grounds for processing of personal data without consent in certain cases.

Processing of personal data necessary for purposes related to employment, etc.

(c) verifying the attendance of the data principal who is an employee of the data fiduciary; or

(d) any other activity relating to the assessment of the performance of the data principal who is an employee of the data fiduciary.

5 (2) Any personal data, not being sensitive personal data, may be processed under sub-section (1), where the consent of the data principal is not appropriate having regard to the employment relationship between the data fiduciary and the data principal, or would involve a disproportionate effort on the part of the data fiduciary due to the nature of the processing under the said sub-section.

10 **14. (1)** In addition to the grounds referred to under sections 12 and 13, the personal data may be processed without obtaining consent under section 11, if such processing is necessary for such reasonable purposes as may be specified by regulations, after taking into consideration—

(a) the interest of the data fiduciary in processing for that purpose;

15 (b) whether the data fiduciary can reasonably be expected to obtain the consent of the data principal;

(c) any public interest in processing for that purpose;

(d) the effect of the processing activity on the rights of the data principal; and

20 (e) the reasonable expectations of the data principal having regard to the context of the processing.

(2) For the purpose of sub-section (1), the expression "reasonable purposes" may include—

(a) prevention and detection of any unlawful activity including fraud;

(b) whistle blowing;

25 (c) mergers and acquisitions;

(d) network and information security;

(e) credit scoring;

(f) recovery of debt;

(g) processing of publicly available personal data; and

30 (h) the operation of search engines.

(3) Where the Authority specifies a reasonable purpose under sub-section (1), it shall—

(a) lay down, by regulations, such safeguards as may be appropriate to ensure the protection of the rights of data principals; and

40 (b) determine where the provision of notice under section 7 shall apply or not apply having regard to the fact whether such provision shall substantially prejudice the relevant reasonable purpose.

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", having regard to—

(a) the risk of significant harm that may be caused to the data principal by the processing of such category of personal data;

(b) the expectation of confidentiality attached to such category of personal data;

Processing of personal data for other reasonable purposes.

Categorisation of personal data as sensitive personal data.

(c) whether a significantly discernible class of data principals may suffer significant harm from the processing of such category of personal data; and

(d) the adequacy of protection afforded by ordinary provisions applicable to personal data.

(2) The Authority may specify, by regulations, the additional safeguards or restrictions for the purposes of repeated, continuous or systematic collection of sensitive personal data for profiling of such personal data. 5

CHAPTER IV

PERSONAL DATA AND SENSITIVE PERSONAL DATA OF CHILDREN

Processing of personal data and sensitive personal data of children.

16. (1) Every data fiduciary shall process personal data of a child in such manner that 10 protects the rights of, and is in the best interests of, the child.

(2) The data fiduciary shall, before processing of any personal data of a child, verify his age and obtain the consent of his parent or guardian, in such manner as may be specified by regulations.

(3) The manner for verification of the age of child under sub-section (2) shall be 15 specified by regulations, taking into consideration—

- (a) the volume of personal data processed;
- (b) the proportion of such personal data likely to be that of child;
- (c) possibility of harm to child arising out of processing of personal data; and
- (d) such other factors as may be prescribed. 20

(4) The Authority shall, by regulations, classify any data fiduciary, as guardian data fiduciary, who—

- (a) operate commercial websites or online services directed at children; or
- (b) process large volumes of personal data of children.

(5) The guardian data fiduciary shall be barred from profiling, tracking or behaviourally monitoring of, or targeted advertising directed at, children and undertaking any other processing of personal data that can cause significant harm to the child. 25

(6) The provisions of sub-section (5) shall apply in such modified form to the data fiduciary offering counselling or child protection services to a child, as the Authority may by regulations specify. 30

(7) A guardian data fiduciary providing exclusive counselling or child protection services to a child shall not require to obtain the consent of parent or guardian of the child under sub-section (2).

Explanation.—For the purposes of this section, the expression "guardian data fiduciary" means any data fiduciary classified as a guardian data fiduciary under sub-section (4). 35

CHAPTER V

RIGHTS OF DATA PRINCIPAL

Right to confirmation and access.

17. (1) The data principal shall have the right to obtain from the data fiduciary—

(a) confirmation whether the data fiduciary is processing or has processed personal data of the data principal; 40

(b) the personal data of the data principal being processed or that has been processed by the data fiduciary, or any summary thereof;

(c) a brief summary of processing activities undertaken by the data fiduciary with respect to the personal data of the data principal, including any information provided in the notice under section 7 in relation to such processing.

5 (2) The data fiduciary shall provide the information under sub-section (1) to the data principal in a clear and concise manner that is easily comprehensible to a reasonable person.

(3) The data principal shall have the right to access in one place the identities of the data fiduciaries with whom his personal data has been shared by any data fiduciary together with the categories of personal data shared with them, in such manner as may be specified by regulations.

10 18. (1) The data principal shall where necessary, having regard to the purposes for which personal data is being processed, subject to such conditions and in such manner as may be specified by regulations, have the right to—

(a) the correction of inaccurate or misleading personal data;

(b) the completion of incomplete personal data;

15 (c) the updating of personal data that is out-of-date; and

(d) the erasure of personal data which is no longer necessary for the purpose for which it was processed.

20 (2) Where the data fiduciary receives a request under sub-section (1), and the data fiduciary does not agree with such correction, completion, upation or erasure having regard to the purposes of processing, such data fiduciary shall provide the data principal with adequate justification in writing for rejecting the application.

25 (3) Where the data principal is not satisfied with the justification provided by the data fiduciary under sub-section (2), the data principal may require that the data fiduciary take reasonable steps to indicate, alongside the relevant personal data, that the same is disputed by the data principal.

30 (4) Where the data fiduciary corrects, completes, updates or erases any personal data in accordance with sub-section (1), such data fiduciary shall also take necessary steps to notify all relevant entities or individuals to whom such personal data may have been disclosed regarding the relevant correction, completion, upation or erasure, particularly where such action may have an impact on the rights and interests of the data principal or on decisions made regarding them.

19. (1) Where the processing has been carried out through automated means, the data principal shall have the right to—

35 (a) receive the following personal data in a structured, commonly used and machine-readable format—

(i) the personal data provided to the data fiduciary;

(ii) the data which has been generated in the course of provision of services or use of goods by the data fiduciary; or

40 (iii) the data which forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained; and

(b) have the personal data referred to in clause (a) transferred to any other data fiduciary in the format referred to in that clause.

(2) The provisions of sub-section (1) shall not apply where—

45 (a) processing is necessary for functions of the State or in compliance of law or order of a court under section 12;

(b) compliance with the request in sub-section (1) would reveal a trade secret of any data fiduciary or would not be technically feasible.

Right to correction and erasure.

Right to data portability.

Right to be forgotten.

20. (1) The data principal shall have the right to restrict or prevent the continuing disclosure of his personal data by a data fiduciary where such disclosure—

(a) has served the purpose for which it was collected or is no longer necessary for the purpose;

(b) was made with the consent of the data principal under section 11 and such consent has since been withdrawn; or

(c) was made contrary to the provisions of this Act or any other law for the time being in force.

(2) The rights under sub-section (1) may be enforced only on an order of the Adjudicating Officer made on an application filed by the data principal, in such form and manner as may be prescribed, on any of the grounds specified under clauses (a), (b) or clause (c) of that sub-section:

Provided that no order shall be made under this sub-section unless it is shown by the data principal that his right or interest in preventing or restricting the continued disclosure of his personal data overrides the right to freedom of speech and expression and the right to information of any other citizen.

(3) The Adjudicating Officer shall, while making an order under sub-section (2), having regard to—

(a) the sensitivity of the personal data;

(b) the scale of disclosure and the degree of accessibility sought to be restricted or prevented;

(c) the role of the data principal in public life;

(d) the relevance of the personal data to the public; and

(e) the nature of the disclosure and of the activities of the data fiduciary, particularly whether the data fiduciary systematically facilitates access to personal data and whether the activities shall be significantly impeded if disclosures of the relevant nature were to be restricted or prevented.

(4) Where any person finds that personal data, the disclosure of which has been restricted or prevented by an order of the Adjudicating Officer under sub-section (2), does not satisfy the conditions referred to in that sub-section, he may apply for the review of that order to the Adjudicating Officer in such manner as may be prescribed, and the Adjudicating Officer shall review his order.

(5) Any person aggrieved by an order made under this section by the Adjudicating Officer may prefer an appeal to the Appellate Tribunal.

General conditions for the exercise of rights in this Chapter.

21. (1) The data principal, for exercising any right under this Chapter, except the right under section 20, shall make a request in writing to the data fiduciary either directly or through a consent manager with the necessary information as regard to his identity, and the data fiduciary shall acknowledge the receipt of such request within such period as may be specified by regulations.

(2) For complying with the request made under sub-section (1), the data fiduciary may charge such fee as may be specified by regulations:

Provided that no fee shall be required for any request in respect of rights referred to in clause (a) or (b) of sub-section (1) of section 17 or section 18.

(3) The data fiduciary shall comply with the request under this Chapter and communicate the same to the data principal, within such period as may be specified by regulations.

(4) Where any request made under this Chapter is refused by the data fiduciary, it shall provide the data principal the reasons in writing for such refusal and shall inform the data

5

10

15

20

25

30

35

40

45

principal regarding the right to file a complaint with the Authority against the refusal, within such period and in such manner as may be specified by regulations.

(5) The data fiduciary is not obliged to comply with any request under this Chapter where such compliance shall harm the rights of any other data principal under this Act.

5

CHAPTER VI

TRANSPARENCY AND ACCOUNTABILITY MEASURES

22. (1) Every data fiduciary shall prepare a privacy by design policy, containing—

Privacy by
design policy.

(a) the managerial, organisational, business practices and technical systems designed to anticipate, identify and avoid harm to the data principal;

10

(b) the obligations of data fiduciaries;

(c) the technology used in the processing of personal data is in accordance with commercially accepted or certified standards;

(d) the legitimate interests of businesses including any innovation is achieved without compromising privacy interests;

15

(e) the protection of privacy throughout processing from the point of collection to deletion of personal data;

(f) the processing of personal data in a transparent manner; and

(g) the interest of the data principal is accounted for at every stage of processing of personal data.

20

(2) Subject to the regulations made by the Authority, the data fiduciary may submit its privacy by design policy prepared under sub-section (1) to the Authority for certification within such period and in such manner as may be specified by regulations.

(3) The Authority, or an officer authorised by it, shall certify the privacy by design policy on being satisfied that it complies with the requirements of sub-section (1).

25

(4) The privacy by design policy certified under sub-section (3) shall be published on the website of the data fiduciary and the Authority.

30

23. (1) Every data fiduciary shall take necessary steps to maintain transparency in processing personal data and shall make the following information available in such form and manner as may be specified by regulations—

Transparency
in processing
of personal
data.

(a) the categories of personal data generally collected and the manner of such collection;

(b) the purposes for which personal data is generally processed;

(c) any categories of personal data processed in exceptional situations or any exceptional purposes of processing that create a risk of significant harm;

35

(d) the existence of and the procedure for exercise of rights of data principal under Chapter V and any related contact details for the same;

(e) the right of data principal to file complaint against the data fiduciary to the Authority;

40

(f) where applicable, any rating in the form of a data trust score that may be accorded to the data fiduciary under sub-section (5) of section 29;

(g) where applicable, information regarding cross-border transfers of personal data that the data fiduciary generally carries out; and

(h) any other information as may be specified by regulations.

(2) The data fiduciary shall notify, from time to time, the important operations in the processing of personal data related to the data principal in such manner as may be specified by regulations.

(3) The data principal may give or withdraw his consent to the data fiduciary through a consent manager. 5

(4) Where the data principal gives or withdraws consent to the data fiduciary through a consent manager, such consent or its withdrawal shall be deemed to have been communicated directly by the data principal.

(5) The consent manager under sub-section (3), shall be registered with the Authority in such manner and subject to such technical, operational, financial and other conditions as may be specified by regulations. 10

Explanation.—For the purposes of this section, a "consent manager" is a data fiduciary which enables a data principal to gain, withdraw, review and manage his consent through an accessible, transparent and interoperable platform.

24. (1) Every data fiduciary and the data processor shall, having regard to the nature, scope and purpose of processing personal data, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, implement necessary security safeguards, including— 15

(a) use of methods such as de-identification and encryption;

(b) steps necessary to protect the integrity of personal data; and 20

(c) steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data.

(2) Every data fiduciary and data processor shall undertake a review of its security safeguards periodically in such manner as may be specified by regulations and take appropriate measures accordingly. 25

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.

(2) The notice referred to in sub-section (1) shall include the following particulars, namely:— 30

(a) nature of personal data which is the subject-matter of the breach;

(b) number of data principals affected by the breach;

(c) possible consequences of the breach; and

(d) action being taken by the data fiduciary to remedy the breach.

(3) The notice referred to in sub-section (1) shall be made by the data fiduciary to the Authority as soon as possible and within such period as may be specified by regulations, following the breach after accounting for any period that may be required to adopt any urgent measures to remedy the breach or mitigate any immediate harm. 35

(4) Where it is not possible to provide all the information specified in sub-section (2) at the same time, the data fiduciary shall provide such information to the Authority in phases without undue delay. 40

(5) Upon receipt of a notice, the Authority shall determine whether such breach should be reported by the data fiduciary to the data principal, taking into account the severity of the harm that may be caused to such data principal or whether some action is required on the part of the data principal to mitigate such harm. 45

(6) The Authority may, in addition to requiring the data fiduciary to report the personal data breach to the data principal under sub-section (5), direct the data fiduciary to take appropriate remedial action as soon as possible and to conspicuously post the details of the personal data breach on its website.

5 (7) The Authority may, in addition, also post the details of the personal data breach on its website.

26. (1) The Authority shall, having regard to the following factors, notify any data fiduciary or class of data fiduciary as significant data fiduciary, namely:—

- 10 (a) volume of personal data processed;
- (b) sensitivity of personal data processed;
- (c) turnover of the data fiduciary;
- (d) risk of harm by processing by the data fiduciary;
- (e) use of new technologies for processing; and
- (f) any other factor causing harm from such processing.

15 (2) The data fiduciary or class of data fiduciary referred to in sub-section (1) shall register itself with the Authority in such manner as may be specified by regulations.

20 (3) Notwithstanding anything in this Act, if the Authority is of the opinion that any processing by any data fiduciary or class of data fiduciary carries a risk of significant harm to any data principal, it may, by notification, apply all or any of the obligations specified in sections 27 to 30 to such data fiduciary or class of data fiduciary as if it is a significant data fiduciary.

25 (4) Notwithstanding anything contained in this section, any social media intermediary,—
 (i) with users above such threshold as may be notified by the Central Government, in consultation with the Authority; and
 (ii) whose actions have, or are likely to have a significant impact on electoral democracy, security of the State, public order or the sovereignty and integrity of India, shall be notified by the Central Government, in consultation with the Authority, as a significant data fiduciary:

30 Provided that different thresholds may be notified for different classes of social media intermediaries.

Explanation.—For the purposes of this sub-section, a "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,—

35 (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 on-line storage services.

27. (1) Where the significant data fiduciary intends to undertake any processing involving new technologies or large scale profiling or use of sensitive personal data such as genetic data or biometric data, or any other processing which carries a risk of significant harm to data principals, such processing shall not be commenced unless the data fiduciary has undertaken a data protection impact assessment in accordance with the provisions of this section.

Classification of data fiduciaries as significant data fiduciaries.

Data protection impact assessment.

(2) The Authority may, by regulations specify, such circumstances, or class of data fiduciary, or processing operation where such data protection impact assessment shall be mandatory, and also specify the instances where a data auditor under this Act shall be engaged by the data fiduciary to undertake a data protection impact assessment.

(3) A data protection impact assessment shall, *inter alia*, contain— 5

(a) detailed description of the proposed processing operation, the purpose of processing and the nature of personal data being processed;

(b) assessment of the potential harm that may be caused to the data principals whose personal data is proposed to be processed; and

(c) measures for managing, minimising, mitigating or removing such risk of harm. 10

(4) Upon completion of the data protection impact assessment, the data protection officer appointed under sub-section (1) of section 30, shall review the assessment and submit the assessment with his finding to the Authority in such manner as may be specified by regulations.

(5) On receipt of the assessment and its review, if the Authority has reason to believe that the processing is likely to cause harm to the data principals, the Authority may direct the data fiduciary to cease such processing or direct that such processing shall be subject to such conditions as the Authority may deem fit. 15

Maintenance of records. 28. (1) The significant data fiduciary shall maintain accurate and up-to-date records of the following, in such form and manner as may be specified by regulations, namely:— 20

(a) important operations in the data life-cycle including collection, transfers, and erasure of personal data to demonstrate compliance as required under section 10;

(b) periodic review of security safeguards under section 24;

(c) data protection impact assessments under section 27; and

(d) any other aspect of processing as may be specified by regulations. 25

(2) Notwithstanding anything contained in this Act, this section shall also apply to the State.

(3) Every social media intermediary which is notified as a significant data fiduciary under sub-section (4) of section 26 shall enable the users who register their service from India, or use their services in India, to voluntarily verify their accounts in such manner as may be prescribed. 30

(4) Any user who voluntarily verifies his account shall be provided with such demonstrable and visible mark of verification, which shall be visible to all users of the service, in such manner as may be prescribed.

Audit of policies and conduct of processing, etc. 29. (1) The significant data fiduciary shall have its policies and the conduct of its processing of personal data audited annually by an independent data auditor under this Act. 35

(2) The data auditor shall evaluate the compliance of the data fiduciary with the provisions of this Act, including—

(a) clarity and effectiveness of notices under section 7;

(b) effectiveness of measures adopted under section 22; 40

(c) transparency in relation to processing activities under section 23;

(d) security safeguards adopted pursuant to section 24;

(e) instances of personal data breach and response of the data fiduciary, including the promptness of notice to the Authority under section 25;

(f) timely implementation of processes and effective adherence to obligations under sub-section (3) of section 28; and

(g) any other matter as may be specified by regulations.

(3) The Authority shall specify, by regulations, the form and procedure for conducting 5 audits under this section.

(4) The Authority shall register in such manner, the persons with expertise in the area of information technology, computer systems, data science, data protection or privacy, possessing such qualifications, experience and eligibility having regard to factors such as independence, integrity and ability, as it may be specified by regulations, as data auditors 10 under this Act.

(5) A data auditor may assign a rating in the form of a data trust score to the data fiduciary pursuant to a data audit conducted under this section.

(6) The Authority shall, by regulations, specify the criteria for assigning a rating in the form of a data trust score having regard to the factors mentioned in sub-section (2).

15 (7) Notwithstanding anything contained in sub-section (1), where the Authority is of the view that the data fiduciary is processing personal data in such manner that is likely to cause harm to a data principal, the Authority may direct the data fiduciary to conduct an audit and shall appoint a data auditor for that purpose.

30. (1) Every significant data fiduciary shall appoint a data protection officer possessing 20 such qualification and experience as may be specified by regulations for carrying out the following functions—

Data
protection
officer.

(a) providing information and advice to the data fiduciary on matters relating to fulfilling its obligations under this Act;

25 (b) monitoring personal data processing activities of the data fiduciary to ensure that such processing does not violate the provisions of this Act;

(c) providing advice to the data fiduciary on carrying out the data protection impact assessments, and carry out its review under sub-section (4) of section 27;

(d) providing advice to the data fiduciary on the development of internal mechanisms to satisfy the principles specified under section 22;

30 (e) providing assistance to and co-operating with the Authority on matters of compliance of the data fiduciary with the provisions under this Act;

(f) act as the point of contact for the data principal for the purpose of grievances redressal under section 32; and

35 (g) maintaining an inventory of records to be maintained by the data fiduciary under section 28.

(2) Nothing contained in sub-section (1) shall prevent the data fiduciary from assigning any other function to the data protection officer, which it may consider necessary.

(3) The data protection officer appointed under sub-section (1) shall be based in India and shall represent the data fiduciary under this Act.

40 **31. (1)** The data fiduciary shall not engage, appoint, use or involve a data processor to process personal data on its behalf without a contract entered into by the data fiduciary and such data processor.

Processing by
entities other
than data
fiduciaries.

45 (2) The data processor referred to in sub-section (1) shall not engage, appoint, use, or involve another data processor in the processing on its behalf, except with the authorisation of the data fiduciary and unless permitted in the contract referred to in sub-section (1).

(3) The data processor, and any employee of the data fiduciary or the data processor, shall only process personal data in accordance with the instructions of the data fiduciary and treat it confidential.

Grievance redressal by data fiduciary.

32. (1) Every data fiduciary shall have in place the procedure and effective mechanisms to redress the grievances of data principals efficiently and in a speedy manner. 5

(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, 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. 10

(3) A complaint made under sub-section (2) shall be resolved by the data fiduciary in an expeditious manner and not later than thirty days from the date of receipt of the complaint by such data fiduciary.

(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. 15

CHAPTER VII

RESTRICTION ON TRANSFER OF PERSONAL DATA OUTSIDE INDIA

Prohibition on processing of sensitive personal data and critical personal data outside India

33. (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. 20

(2) The critical personal data shall only be processed in India.

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. 25

Conditions for transfer of sensitive personal data and critical personal data.

34. (1) The sensitive personal data may only be transferred outside India for the purpose of processing, when explicit consent is given by the data principal for such transfer, and where—

(a) the transfer is made pursuant to a contract or intra-group scheme approved by the Authority; 30

Provided that such contract or intra-group scheme shall not be approved, unless it makes the provisions for—

(i) effective protection of the rights of the data principal under this Act, including in relation to further transfer to any other person; and 35

(ii) liability of the data fiduciary for harm caused due to non-compliance of the provisions of such contract or intra-group scheme by such transfer; or

(b) the Central Government, after consultation with the Authority, has allowed the transfer to a country or, such entity or class of entity in a country or, an international organisation on the basis of its finding that— 40

(i) such sensitive personal data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements; and

(ii) such transfer shall not prejudicially affect the enforcement of relevant laws by authorities with appropriate jurisdiction:

Provided that any finding under this clause shall be reviewed periodically in such manner as may be prescribed;

5 (c) the Authority has allowed transfer of any sensitive personal data or class of sensitive personal data necessary for any specific purpose.

(2) Notwithstanding anything contained in sub-section (2) of section 33, any critical personal data may be transferred outside India, only where such transfer is—

10 (a) to a person or entity engaged in the provision of health services or emergency services where such transfer is necessary for prompt action under section 12; or

15 (b) to a country or, any entity or class of entity in a country or, to an international organisation, where the Central Government has deemed such transfer to be permissible under clause (b) of sub-section (I) and where such transfer in the opinion of the Central Government does not prejudicially affect the security and strategic interest of the State.

(3) Any transfer under clause (a) of sub-section (2) shall be notified to the Authority within such period as may be specified by regulations.

CHAPTER VIII

EXEMPTIONS

20 **35.** Where the Central Government is satisfied that it is necessary or expedient,—

Power of
Central
Government
to exempt
any agency of
Government
from
application of
Act.

(i) in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order; or

25 (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.

30 *Explanation.*—For the purposes of this section,—

2 of 1974. (i) the term "cognizable offence" means the offence as defined in clause (c) of section 2 of the Code of Criminal Procedure, 1973;

35 (ii) the expression "processing of such personal data" includes sharing by or sharing with such agency of the Government by any data fiduciary, data processor or data principal.

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—

Exemption of
certain
provisions for
certain
processing of
personal data.

40 (a) personal data is processed in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of any law for the time being in force;

(b) disclosure of personal data is necessary for enforcing any legal right or claim, seeking any relief, defending any charge, opposing any claim, or obtaining any legal advice from an advocate in any impending legal proceeding;

(c) processing of personal data by any court or tribunal in India is necessary for the exercise of any judicial function; 5

(d) personal data is processed by a natural person for any personal or domestic purpose, except where such processing involves disclosure to the public, or is undertaken in connection with any professional or commercial activity; or

(e) processing of personal data is necessary for or relevant to a journalistic purpose, by any person and is in compliance with any code of ethics issued by the Press Council of India, or by any media self-regulatory organisation. 10

37. The Central Government may, by notification, exempt from the application of this Act, the processing of personal data of data principals not within the territory of India, pursuant to any contract entered into with any person outside the territory of India, including any company incorporated outside the territory of India, by any data processor or any class of data processors incorporated under Indian law. 15

38. Where the processing of personal data is necessary for research, archiving, or statistical purposes, and the Authority is satisfied that—

(a) the compliance with the provisions of this Act shall disproportionately divert resources from such purpose; 20

(b) the purposes of processing cannot be achieved if the personal data is anonymised;

(c) the data fiduciary has carried out de-identification in accordance with the code of practice specified under section 50 and the purpose of processing can be achieved if the personal data is in de-identified form; 25

(d) the personal data shall not be used to take any decision specific to or action directed to the data principal; and

(e) the personal data shall not be processed in the manner that gives rise to a risk of significant harm to the data principal,

it may, by notification, exempt such class of research, archiving, or statistical purposes from the application of any of the provisions of this Act as may be specified by regulations. 30

39. (1) The provisions of sections 7, 8, 9, clause (c) of sub-section (1) of section 17 and sections 19 to 32 shall not apply where the processing of personal data by a small entity is not automated.

(2) For the purposes of sub-section (1), a "small entity" means such data fiduciary as may be classified, by regulations, by Authority, having regard to— 35

(a) the turnover of data fiduciary in the preceding financial year;

(b) the purpose of collection of personal data for disclosure to any other individuals or entities; and

(c) the volume of personal data processed by such data fiduciary in any one day in the preceding twelve calendar months. 40

40. (1) The Authority shall, for the purposes of encouraging innovation in artificial intelligence, machine-learning or any other emerging technology in public interest, create a Sandbox.

Power of
Central
Government
to exempt
certain data
processors.

Exemption
for research,
archiving or
statistical
purposes.

Exemption
for manual
processing by
small entities.

Sandbox for
encouraging
innovation,
etc.

(2) Any data fiduciary whose privacy by design policy is certified by the Authority under sub-section (3) of section 22 shall be eligible to apply, in such manner as may be specified by regulations, for inclusion in the Sandbox created under sub-section (1).

5 (3) Any data fiduciary applying for inclusion in the Sandbox under sub-section (2) shall furnish the following information, namely:—

10 (a) the term for which it seeks to utilise the benefits of Sandbox, provided that such term shall not exceed twelve months;

(b) the innovative use of technology and its beneficial uses;

15 (c) the data principals or categories of data principals participating under the proposed processing; and

(d) any other information as may be specified by regulations.

(4) The Authority shall, while including any data fiduciary in the Sandbox, specify—

15 (a) the term of the inclusion in the Sandbox, which may be renewed not more than twice, subject to a total period of thirty-six months;

20 (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 licensed activity, compensation to such data principals and penalties in relation to such safeguards; and

(c) that the following obligations shall not apply or apply with modified form to such data fiduciary, namely:—

(i) the obligation to specify clear and specific purposes under sections 4 and 5;

(ii) limitation on collection of personal data under section 6; and

25 (iii) any other obligation to the extent, it is directly depending on the obligations under sections 5 and 6; and

(iv) the restriction on retention of personal data under section 9.

CHAPTER IX

DATA PROTECTION AUTHORITY OF INDIA

30 **41. (1)** The Central Government shall, by notification, establish, for the purposes of this Act, an Authority to be called the Data Protection Authority of India.

Establishment
of Authority.

(2) The Authority referred to in sub-section (1) shall be a body corporate by the name aforesaid, having perpetual succession and a common seal, with power, subject to the provisions of this Act, to acquire, hold and dispose of property, both movable and immovable, 35 and to contract and shall, by the said name, sue or be sued.

(3) The head office of the Authority shall be at such place as may be prescribed.

(4) The Authority may, with the prior approval of the Central Government, establish its offices at other places in India.

40 **42. (1)** The Authority shall consist of a Chairperson and not more than six whole-time Members, of which one shall be a person having qualification and experience in law.

Composition
and
qualifications
for
appointment
of Members.

(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—

(a) the Cabinet Secretary, who shall be Chairperson of the selection committee;

45 (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.

(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.

(4) The Chairperson and the Members of the Authority shall be persons of ability, integrity and standing, and shall have qualification and specialised 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. 5

(5) A vacancy caused to the office of the Chairperson or any other member of the Authority shall be filled up within a period of three months from the date on which such vacancy occurs. 10

43. (1) The Chairperson and the Members of the Authority shall be appointed for a term of five years or till they attain the age of sixty-five years, whichever is earlier, and they shall not be eligible for re-appointment. 15

(2) The salaries and allowances payable to, and other terms and conditions of service of the Chairperson and the Members of the Authority shall be such as may be prescribed.

(3) The Chairperson and the Members shall not, during their term and for a period of two years from the date on which they cease to hold office, accept—

(a) any employment either under the Central Government or under any State Government; or 20

(b) any appointment, in any capacity whatsoever, with a significant data fiduciary.

(4) Notwithstanding anything contained in sub-section (1), the Chairperson or a Member of the Authority may—

(a) relinquish his office by giving in writing to the Central Government a notice of not less than three months; or 25

(b) be removed from his office in accordance with the provisions of this Act.

44. (1) The Central Government may remove from office, the Chairperson or any Member of the Authority who—
other
Members.

(a) has been adjudged as an insolvent; 30

(b) has become physically or mentally incapable of acting as a Chairperson or member;

(c) has been convicted of an offence, which in the opinion of the Central Government, involves moral turpitude;

(d) has so abused their position as to render their continuation in office detrimental to the public interest; or 35

(e) has acquired such financial or other interest as is likely to affect prejudicially their functions as a Chairperson or a member.

(2) No Chairperson or any member of the Authority shall be removed under clause (d) or (e) of sub-section (1) unless he has been given a reasonable opportunity of being heard. 40

45. The Chairperson of the Authority shall have powers of general superintendence and direction of the affairs of the Authority and shall also exercise all powers and do all such acts and things which may be exercised or done by the Authority under this Act.

- 46.** (1) The Chairperson and Members of the Authority shall meet at such times and places and shall observe such rules and procedures in regard to transaction of business at its meetings including quorum at such meetings, as may be prescribed. Meetings of Authority.
- (2) If, for any reason, the Chairperson is unable to attend any meeting of the Authority, 5 any other member chosen by the Members present at the meeting, shall preside the meeting.
- (3) All questions which come up before any meeting of the Authority shall be decided by a majority of votes of the Members present and voting, and in the event of an equality of votes, the Chairperson or in his absence, the member presiding, shall have the right to exercise a second or casting vote.
- 10 (4) Any Member who has any direct or indirect pecuniary interest in any matter coming up for consideration at a meeting of the Authority shall disclose the nature of his interest at such meeting, which shall be recorded in the proceedings of the Authority and such member shall not take part in any deliberation or decision of the Authority with respect to that matter.
- 47.** No act or proceeding of the Authority shall be invalid merely by reason of— Vacancies, etc., not to invalidate proceedings of Authority.
- 15 (a) any vacancy or defect in the constitution of the Authority;
- (b) any defect in the appointment of a person as a Chairperson or member; or
- (c) any irregularity in the procedure of the Authority not affecting the merits of the case.
- 48.** (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. Officers and other employees of Authority.
- (2) Any remuneration, salary or allowances, and other terms and conditions of service of such officers, employees, consultants and experts shall be such as may be specified by regulations.
- 25 **49.** (1) It shall be the duty of the Authority to protect the interests of data principals, prevent any misuse of personal data, ensure compliance with the provisions of this Act, and promote awareness about data protection. Powers and functions of Authority.
- (2) Without prejudice to the generality of the foregoing and other functions under this Act, the functions of the Authority shall include—
- 30 (a) monitoring and enforcing application of the provisions of this Act;
- (b) taking prompt and appropriate action in response to personal data breach in accordance with the provisions of this Act;
- (c) maintaining a database on its website containing names of significant data fiduciaries along with a rating in the form of a data trust score indicating compliance with the obligations of this Act by such fiduciaries;
- 35 (d) examination of any data audit reports and taking any action pursuant thereto;
- (e) issuance of a certificate of registration to data auditors and renewal, withdrawal, suspension or cancellation thereof and maintaining a database of registered data auditors and specifying the qualifications, code of conduct, practical training and functions to be performed by such data auditors;
- 40 (f) classification of data fiduciaries;
- (g) monitoring cross-border transfer of personal data;
- (h) specifying codes of practice;

(i) promoting awareness and understanding of the risks, rules, safeguards and rights in respect of protection of personal data amongst data fiduciaries and data principals;

(j) monitoring technological developments and commercial practices that may affect protection of personal data; 5

(k) promoting measures and undertaking research for innovation in the field of protection of personal data;

(l) advising Central Government, State Government and any other authority on measures required to be taken to promote protection of personal data and ensuring consistency of application and enforcement of this Act; 10

(m) specifying fees and other charges for carrying out the purposes of this Act;

(n) receiving and inquiring complaints under this Act; and

(o) performing such other functions as may be prescribed.

(3) Where, pursuant to the provisions of this Act, the Authority processes any personal data, it shall be construed as the data fiduciary or the data processor in relation to such personal data as applicable, and where the Authority comes into possession of any information that is treated as confidential by the data fiduciary or data processor, it shall not disclose such information unless required under any law to do so, or where it is required to carry out its function under this section. 15

Codes of practice. 50. (1) The Authority shall, by regulations, specify codes of practice to promote good practices of data protection and facilitate compliance with the obligations under this Act. 20

(2) Notwithstanding anything contained in sub-section (1), the Authority may approve any code of practice submitted by an industry or trade association, an association representing the interest of data principals, any sectoral regulator or statutory Authority, or any departments or ministries of the Central or State Government. 25

(3) The Authority shall ensure transparency and compliance with the obligations of data fiduciary and the rights of the data principal under this Act while specifying or approving any code of practice under this section.

(4) A code of practice under sub-section (1) or sub-section (2), shall not be issued unless the Authority has made consultation with the sectoral regulators and other stakeholders including the public and has followed such procedure as may be prescribed. 30

(5) A code of practice issued under this section shall not derogate from the provisions of this Act or any other law for the time being in force.

(6) The code of practice under this Act may include the following matters, namely:—

(a) requirements for notice under section 7 including any model forms or guidance relating to notice; 35

(b) measures for ensuring quality of personal data processed under section 8;

(c) measures pertaining to the retention of personal data under section 9;

(d) manner for obtaining valid consent under section 11;

(e) processing of personal data under section 12; 40

(f) activities where processing of personal data may be undertaken under section 14;

(g) processing of sensitive personal data under Chapter III;

(h) processing of personal data under any other ground for processing, including processing of personal data of children and age-verification under this Act; 45

- (i) exercise of any right by data principals under Chapter V;
- (j) the standards and means by which a data principal may avail the right to data portability under section 19;
- 5 (k) transparency and accountability measures including the standards thereof to be maintained by data fiduciaries and data processors under Chapter VI;
- (l) standards for security safeguards to be maintained by data fiduciaries and data processors under section 24;
- (m) methods of de-identification and anonymisation;
- 10 (n) methods of destruction, deletion, or erasure of personal data where required under this Act;
- (o) appropriate action to be taken by the data fiduciary or data processor in response to a personal data breach under section 25;
- (p) manner in which data protection impact assessments may be carried out by the data fiduciary or a class thereof under section 27;
- 15 (q) transfer of personal data outside India pursuant to section 34;
- (r) processing of any personal data or sensitive personal data to carry out any activity necessary for research, archiving or statistical purposes under section 38; and
- (s) any other matter which, in the view of the Authority, may be necessary to be provided in the code of practice.

20 (7) The Authority may review, modify or revoke a code of practice issued under this section in such manner as may be prescribed.

51. (1) The Authority may, for the discharge of its functions under this Act, issue such directions from time to time as it may consider necessary to any data fiduciary or data processor who shall be bound to comply with such directions.

Power of Authority to issue directions.

(2) No direction shall be issued under sub-section (1) unless the Authority has given a reasonable opportunity of being heard to the data fiduciaries or data processor concerned.

30 (3) The Authority may, on a representation made to it or on its own motion, modify, suspend, withdraw or cancel any direction issued under sub-section (1) and in doing so, may impose such conditions as it deems fit, subject to which the modification, suspension, withdrawal or cancellation shall have effect.

Power of Authority to call for information.

52. (1) Without prejudice to the other provisions of this Act, the Authority may require a data fiduciary or data processor to provide such information as may be reasonably required by it for discharging its functions under this Act.

35 (2) If the Authority requires a data fiduciary or a data processor to provide any information under sub-section (1), it shall provide a notice in writing to the data fiduciary or the data processor stating the reasons for such requisition.

(3) The Authority shall, by regulations, specify the manner in which the data fiduciary or data processor shall provide the information sought in sub-section (1), including the designation of the officer or employee of the Authority who may seek such information, the period within which such information is to be furnished and the form in which such information may be provided.

Power of Authority to conduct inquiry.

53. (1) The Authority may, on its own or on a complaint received by it, inquire or cause to be inquired, if it has reasonable grounds to believe that—

45 (a) the activities of the data fiduciary or data processor are being conducted in a manner which is detrimental to the interest of data principals; or

(b) any data fiduciary or data processor has contravened any of the provisions of this Act or the rules or regulations made thereunder, or any direction of the Authority.

(2) For the purposes of sub-section (1), the Authority shall, by an order in writing, appoint one of its officers as an Inquiry Officer to inquire into the affairs of such data fiduciary or data processor and to report to the Authority on any inquiry made. 5

(3) For the purpose of any inquiry under this section, the Inquiry Officer may, wherever necessary, seek the assistance of any other person.

(4) The order referred to in sub-section (2) shall specify the reasons for the inquiry and the scope of the inquiry and may be modified from time to time.

(5) Every officer, employee or other person acting under the direct authority of the data fiduciary or the data processor, or a service provider, or a contractor, where services are being obtained by or provided to the data fiduciary or data processor, as the case may be, shall be bound to produce before the Inquiry Officer, all such books, registers, documents, records and any data in their custody or power and to furnish to the Inquiry Officer any statement and information relating to the affairs of the data fiduciary or data processor as the Inquiry Officer may require within such time as the said Inquiry Officer may specify. 10 15

(6) The Inquiry Officer shall provide a notice in writing to the persons referred to in sub-section (5) stating the reasons thereof and the relationship between the data fiduciary and the Inquiry Officer.

(7) The Inquiry Officer may keep in its custody any books, registers, documents, records and other data produced under sub-section (5) for six months and thereafter shall return the same to the person by whom or on whose behalf such books, registers, documents, record and data are produced, unless an approval to retain such books, registers, documents, record and data for an additional period not exceeding three months has been obtained from the Authority. 20 25

(8) Notwithstanding anything contained in any other law for the time being in force, while exercising the powers under this section, the Authority or the Inquiry Officer, as the case may be, shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 while trying a suit, in respect of the following matters, namely— 5 of 1908.

(a) the discovery and production of books of account and other documents, at such place and at such time as may be specified;

(b) summoning and enforcing the attendance of persons and examining them on oath;

(c) inspection of any book, document, register or record of any data fiduciary;

(d) issuing commissions for the examination of witnesses or documents; and 35

(e) any other matter which may be prescribed.

Action to be taken by Authority pursuant to an inquiry.

54. (1) On receipt of a report under sub-section (2) of section 53, the Authority may, after giving such opportunity to the data fiduciary or data processor to make a representation in connection with the report as the Authority deems reasonable, by an order in writing—

(a) issue a warning to the data fiduciary or data processor where the business or activity is likely to violate the provisions of this Act; 40

(b) issue a reprimand to the data fiduciary or data processor where the business or activity has violated the provisions of this Act;

(c) require the data fiduciary or data processor to cease and desist from committing or causing any violation of the provisions of this Act; 45

(d) require the data fiduciary or data processor to modify its business or activity to bring it in compliance with the provisions of this Act;

(e) temporarily suspend or discontinue business or activity of the data fiduciary or data processor which is in contravention of the provisions of this Act;

(f) vary, suspend or cancel any registration granted by the Authority in case of a significant data fiduciary;

5 (g) suspend or discontinue any cross-border flow of personal data; or

(h) require the data fiduciary or data processor to take any such action in respect of any matter arising out of the report as the Authority may deems fit.

(2) A data fiduciary or data processor aggrieved by an order made under this section may prefer an appeal to the Appellate Tribunal.

10 **55.** (1) Where in the course of inquiry under section 53, the Inquiry Officer has reasonable ground to believe that any books, registers, documents, records or data belonging to any person as mentioned therein, are likely to be tampered with, altered, mutilated, manufactured, falsified or destroyed, the Inquiry Officer may make an application to such designated court, as may be notified by the Central Government, for an order for the seizure
15 of such books, registers, documents and records.

(2) The Inquiry Officer may require the services of any police officer or any officer of the Central Government, or of both, to assist him for the purposes specified in sub-section (1) and it shall be the duty of every such officer to comply with such requisition.

20 (3) After considering the application and hearing the Inquiry Officer, if necessary, the designated court may, by order, authorise the Inquiry Officer—

25 (a) to enter, with such assistance, as may be required, the place or places where such books, registers, documents and records are kept;
(b) to search that place or those places in the manner specified in the order; and
(c) to seize books, registers, documents and records it considers necessary for the purposes of the inquiry.

(4) The Inquiry Officer shall keep in its custody the books, registers, documents and records seized under this section for such period not later than the conclusion of the inquiry as it considers necessary and thereafter shall return the same to the person, from whose custody or power they were seized and inform the designated court of such return.

30 (5) Save as otherwise provided in this section, every search or seizure made under this section shall be carried out in accordance with the provisions of the Code of Criminal Procedure, 1973 relating to searches or seizures made under that Code.

2 of 1974.

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.

Search and seizure.

Co-ordination between Authority and other regulators or authorities.

40

CHAPTER X

PENALTIES AND COMPENSATION

57. (1) Where the data fiduciary contravenes any of the following provisions,—

Penalties for contravening certain provisions of the Act.

(a) obligation to take prompt and appropriate action in response to a data security breach under section 25;

(b) failure to register with the Authority under sub-section (2) of section 26,

(c) obligation to undertake a data protection impact assessment by a significant data fiduciary under section 27;

(d) obligation to conduct a data audit by a significant data fiduciary under section 29;

(e) appointment of a data protection officer by a significant data fiduciary under section 30, 5

it shall be liable to a penalty which may extend to five crore rupees or two per cent. of its total worldwide turnover of the preceding financial year, whichever is higher;

(2) Where a data fiduciary contravenes any of the following provisions,—

(a) processing of personal data in violation of the provisions of Chapter II or 10 Chapter III;

(b) processing of personal data of children in violation of the provisions of Chapter IV;

(c) failure to adhere to security safeguards as per section 24; or

(d) transfer of personal data outside India in violation of the provisions of 15 Chapter VII,

it shall be liable to a penalty which may extend to fifteen crore rupees or four per cent. of its total worldwide turnover of the preceding financial year, whichever is higher.

(3) For the purposes of this section,—

(a) the expression "total worldwide turnover" means the gross amount of 20 revenue recognised in the profit and loss account or any other equivalent statement, as applicable, from the sale, supply or distribution of goods or services or on account of services rendered, or both, and where such revenue is generated within India and outside India.

(b) it is hereby clarified that total worldwide turnover in relation to a data fiduciary 25 is the total worldwide turnover of the data fiduciary and the total worldwide turnover of any group entity of the data fiduciary where such turnover of a group entity arises as a result of the processing activities of the data fiduciary, having regard to factors, including—

(i) the alignment of the overall economic interests of the data fiduciary 30 and the group entity;

(ii) the relationship between the data fiduciary and the group entity specifically in relation to the processing activity undertaken by the data fiduciary; and

(iii) the degree of control exercised by the group entity over the data 35 fiduciary or *vice versa*, as the case may be.

(c) where of any provisions referred to in this section has been contravened by the State, the maximum penalty shall not exceed five crore rupees under sub-section (1), and fifteen crore rupees under sub-section (2), respectively.

58. Where, any data fiduciary, without any reasonable explanation, fails to comply 40 with any request made by a data principal under Chapter V, such data fiduciary shall be liable to a penalty of five thousand rupees for each day during which such default continues, subject to a maximum of ten lakh rupees in case of significant data fiduciaries and five lakh rupees in other cases.

59. If any data fiduciary, who is required under this Act, or the rules or regulations made thereunder, to furnish any report, return or information to the Authority, fails to furnish the same, then such data fiduciary shall be liable to penalty which shall be ten thousand rupees for each day during which such default continues, subject to a maximum of twenty five lakh rupees in case of significant data fiduciaries and five lakh rupees in other cases.

Penalty for failure to furnish report, returns, information, etc.

60. If any data fiduciary or data processor fails to comply with any direction issued by the Authority under section 51 or order issued by the Authority under section 54, such data fiduciary or data processor shall be liable to a penalty which may extend to twenty thousand rupees for each day during which such default continues, subject to a maximum of two crores in case of a data processor it may extend to five thousand rupees for each day during which such default continues, subject to a maximum of fifty lakh rupees.

Penalty for failure to comply with direction or order issued by Authority.

61. Where any person fails to comply with any provision of this Act or the rules or regulations made thereunder applicable to such person, for which no separate penalty has been provided, then, such person shall be liable to a penalty which may extend to a maximum of one crore rupees in case of significant data fiduciaries, and a maximum of twenty five lakh rupees in other cases.

Penalty for contravention where no separate penalty has been provided.

62. (1) For the purpose of adjudging the penalties under sections 57 to 61 or awarding compensation under section 64, the Authority shall appoint such Adjudicating Officer as may be prescribed.

Appointment of Adjudicating Officer.

20 (2) The Central Government shall, having regard to the need to ensure the operational segregation, independence, and neutrality of the adjudication under this Act, prescribe—

(a) number of Adjudicating Officers to be appointed under sub-section (1);

(b) manner and terms of appointment of Adjudicating Officers ensuring independence of such officers;

25 (c) jurisdiction of Adjudicating Officers;

(d) other such requirements as the Central Government may deem fit.

30 (3) The Adjudicating Officers shall be persons of ability, integrity and standing, and must have specialised knowledge of, and not less than seven years professional experience in the fields of law, cyber and internet laws, information technology law and policy, data protection and related subjects.

Procedure for adjudication by Adjudicating Officer.

63. (1) No penalty shall be imposed under this Chapter, except after an inquiry made in such manner as may be prescribed, and the data fiduciary or data processor or any person, as the case may be, has been given a reasonable opportunity of being heard:

35 Provided that no inquiry under this section shall be initiated except by a complaint made by the Authority.

(2) While holding an inquiry, the Adjudicating Officer shall have the power to summon and enforce the attendance of any person acquainted with the facts and circumstances of the case to give evidence or to produce any document which, in the opinion of the Adjudicating Officer, may be useful for or relevant to the subject matter of the inquiry.

40 (3) If, on the conclusion of such inquiry, the Adjudicating Officer is satisfied that the person has failed to comply with the provisions of this Act or has caused harm to any data principal as a result of any contravention of the provisions of this Act, the Adjudicating Officer may impose such penalty specified under relevant section.

45 (4) While deciding whether to impose a penalty under sub-section (3) and in determining the quantum of penalty under sections 57 to 61, the Adjudicating Officer shall have due regard to the following factors, namely:—

(a) nature, gravity and duration of violation taking into account the nature, scope and purpose of processing concerned;

- (b) number of data principals affected, and the level of harm suffered by them;
 - (c) intentional or negligent character of the violation;
 - (d) nature of personal data impacted by the violation;
 - (e) repetitive nature of the default;
 - (f) transparency and accountability measures implemented by the data fiduciary 5 or data processor including adherence to any relevant code of practice relating to security safeguards;
 - (g) action taken by the data fiduciary or data processor to mitigate the harm suffered by data principals; and
 - (h) any other aggravating or mitigating factors relevant to the circumstances of the case, such as, the amount of disproportionate gain or unfair advantage, wherever quantifiable, made as a result of the default. 10
- (5) Any person aggrieved by an order under this section by the Adjudicating Officer may prefer an appeal to the Appellate Tribunal. 15
- Compensation.** 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. 15
- Explanation.*—For the removal of doubts, it is hereby clarified that a data processor shall be liable only where it has acted outside or contrary to the instructions of the data fiduciary pursuant to section 31, or where the data processor is found to have acted in a negligent manner, or where the data processor has not incorporated adequate security safeguards under section 24, or where it has violated any provisions of this Act expressly applicable to it. 20
- (2) The data principal may seek compensation under this section by making a complaint 25 to the Adjudicating Officer in such form and manner as may be prescribed.
- (3) Where there are one or more data principals or any identifiable class of data principals who have suffered harm as a result of any contravention by the same data fiduciary or data processor, one complaint may be instituted on behalf of all such data principals seeking compensation for the harm suffered. 30
- (4) While deciding to award compensation and the amount of compensation under this section, the Adjudicating Officer shall have regard to the following factors, namely:—
- (a) nature, duration and extent of violation of the provisions of the Act, rules prescribed, or regulations specified thereunder;
 - (b) nature and extent of harm suffered by the data principal; 35
 - (c) intentional or negligent character of the violation;
 - (d) transparency and accountability measures implemented by the data fiduciary or the data processor, as the case may be, including adherence to any relevant code of practice relating to security safeguards;
 - (e) action taken by the data fiduciary or the data processor, as the case may be, 40 to mitigate the damage suffered by the data principal;
 - (f) previous history of any, or such, violation by the data fiduciary or the data processor, as the case may be;
 - (g) whether the arrangement between the data fiduciary and data processor contains adequate transparency and accountability measures to safeguard the personal data being processed by the data processor on behalf of the data fiduciary; 45

(h) any other aggravating or mitigating factor relevant to the circumstances of the case, such as, the amount of disproportionate gain or unfair advantage, wherever quantifiable, made as a result of the default.

(5) Where more than one data fiduciary or data processor, or both a data fiduciary and 5 a data processor are involved in the same processing activity and are found to have caused harm to the data principal, then, each data fiduciary or data processor may be ordered to pay the entire compensation for the harm to ensure effective and speedy compensation to the data principal.

(6) Where a data fiduciary or a data processor has, in accordance with sub-section (5), 10 paid the entire amount of compensation for the harm suffered by the data principal, such data fiduciary or data processor shall be entitled to claim from the other data fiduciaries or data processors, as the case may be, that amount of compensation corresponding to their part of responsibility for the harm caused.

(7) Any person aggrieved by an order made under this section by the Adjudicating 15 Officer may prefer an appeal to the Appellate Tribunal.

(8) The Central Government may prescribe the procedure for hearing of a complaint under this section.

65. No compensation awarded, or penalty imposed, under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under this Act or 20 any other law for the time being in force.

Compensation or penalties not to interfere with other punishment.

66. (1) The amount of any penalty imposed or compensation awarded under this Act, if not paid, may be recovered as if it were an arrear of land revenue.

Recovery of amounts.

(2) All sums realised by way of penalties under this Act shall be credited to the Consolidated Fund of India.

APPELLATE TRIBUNAL

67. (1) The Central Government shall, by notification, establish an Appellate Tribunal to—

Establishment of Appellate Tribunal.

(a) hear and dispose of any appeal from an order of the Adjudicating Officer 30 under sub-section (5) of section 20;

(b) hear and dispose of any appeal from an order of the Authority under sub-section (2) of section 54;

(c) hear and dispose of any appeal from an order of the Adjudicating Officer under sub-section (5) of section 63; and

(d) hear and dispose of any appeal from an order of an Adjudicating Officer under sub-section (7) of section 64.

(2) The Appellate Tribunal shall consist of a Chairperson and not more than members to be appointed.

(3) The Appellate Tribunal shall be established at such place or places, as the 40 Central Government may, in consultation with the Chairperson of the Appellate Tribunal, notify.

(4) Notwithstanding anything contained in sub-sections (1) to (3), where, in the opinion of the Central Government, any existing body is competent to discharge the functions of the Appellate Tribunal under this Act, then, the Central Government may notify such body to 45 act as the Appellate Tribunal under this Act.

Qualifications,
appointment,
term,
conditions of
service of
Members.

68. (1) A person shall not be qualified for appointment as the Chairperson or a member of the Appellate Tribunal unless he—

(a) in the case of Chairperson, is, or has been a Judge of the Supreme Court or Chief Justice of a High Court;

(b) in the case of a member, has held the post of Secretary to the Government of India or any equivalent post in the Central Government for a period of not less than two years or a person who is well versed in the field of data protection, information technology, data management, data science, data security, cyber and internet laws or any related subject. 5

(2) The Central Government may prescribe the manner of appointment, term of office, salaries and allowances, resignation, removal and the other terms and conditions of service of the Chairperson and any member of the Appellate Tribunal. 10

Vacancies.

69. If, for reason other than temporary absence, any vacancy occurs in the office of the Chairperson or a member of the Appellate Tribunal, the Central Government shall appoint another person in accordance with the provisions of this Act and the rules prescribed to fill the vacancy and the proceedings may be continued before the Appellate Tribunal from the stage at which the vacancy is filled. 15

Staff of
Appellate
Tribunal.

70. (1) The Central Government shall provide the Appellate Tribunal with such officers and employees as it may deem fit.

(2) The officers and employees of the Appellate Tribunal shall discharge their functions under the general superintendence of its Chairperson. 20

(3) The salaries and allowances and other conditions of service of such officers and employees of the Appellate Tribunal shall be such as may be prescribed.

Distribution of
business
amongst
Benches.

71. (1) Subject to the provisions of this Act, the jurisdiction of the Appellate Tribunal may be exercised by Benches thereof, which shall be constituted by the Chairperson. 25

(2) Where Benches of the Appellate Tribunal are constituted under sub-section (1), the Chairperson may, from time to time, by notification, make provisions as to the distribution of the business of the Appellate Tribunal amongst the Benches, transfer of Members between Benches, and also provide for the matters which may be dealt with by each bench.

(3) On the application of any of the parties and after notice to the parties, and after hearing such of them as the Chairperson may desire to be heard, or on the Chairperson's own motion without such notice, the Chairperson of the Appellate Tribunal may transfer any case pending before one Bench, for disposal, to any other Bench. 30

Appeals to
Appellate
Tribunal.

72. (1) Any person aggrieved by the decision of the Authority, may prefer an appeal to the Appellate Tribunal within a period of thirty days from the receipt of the order appealed against, in such form, verified in such manner and be accompanied by such fee, as may be prescribed: 35

Provided that the Appellate Tribunal may entertain any appeal after the expiry of the said period of thirty days if it is satisfied that there was sufficient cause for not filing it within that period. 40

(2) On receipt of an appeal under this section, the Appellate Tribunal may, after providing the parties to the dispute or appeal, an opportunity of being heard, pass such orders thereon as it deems fit.

(3) The Appellate Tribunal shall send a copy of every order made by it to the parties to the dispute or the appeal and to the Authority, as the case may be. 45

(4) The Appellate Tribunal may, for the purpose of examining the legality or propriety or correctness, of any decision, or order of the Authority or Adjudicating Officer referred to in the appeal preferred under this section, on its own motion or otherwise, call for the records relevant to disposing of such appeal or application and make such orders as it thinks fit.

5 of 1908. 5 **73. (1)** The Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908, but shall be guided by the principles of natural justice and, subject to the other provisions of this Act, the Appellate Tribunal shall have powers to regulate its own procedure.

Procedure and powers of Appellate Tribunal.

10 (2) The Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil 5 of 1908. Procedure, 1908, while trying a suit, in respect of the following matters, namely—

- (a) summoning and enforcing the attendance of any person and examining his on oath;
- (b) requiring the discovery and production of documents;
- 15 (c) receiving evidence on affidavits;
- (d) subject to the provisions of section 123 and section 124 of the Indian Evidence 1 of 1872. Act, 1872, requisitioning any public record or document or a copy of such record or document, from any office;
- (e) issuing commissions for the examination of witnesses or documents;
- 20 (f) reviewing its decisions;
- (g) dismissing an application for default or deciding it, *ex parte*;
- (h) setting aside any order of dismissal of any application for default or any order passed by it, *ex parte*; and
- (i) any other matter which may be prescribed.

25 (3) Every proceeding before the Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 45 of 1860. 2 of 1974. of the Indian Penal Code and the Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

Orders passed by Appellate Tribunal to be executable as a decree.

30 **74. (1)** An order passed by the Appellate Tribunal under this Act shall be executable by the Appellate Tribunal as a decree of civil court, and for this purpose, the Appellate Tribunal shall have all the powers of a civil court.

(2) Notwithstanding anything contained in sub-section (1), the Appellate Tribunal may transmit any order made by it to a civil court having local jurisdiction and such civil court shall execute the order as if it were a decree made by that court.

5 of 1908. 35 **75. (1)** Notwithstanding anything contained in the Code of Civil Procedure, 1908 or in any other law, an appeal shall lie against any order of the Appellate Tribunal, not being an interlocutory order, to the Supreme Court on any substantial question of law.

Appeal to Supreme Court.

(2) No appeal shall lie against any decision or order made by the Appellate Tribunal with the consent of the parties.

40 (3) Every appeal under this section shall be preferred within a period of ninety days from the date of the decision or order appealed against:

Provided that the Supreme Court may entertain the appeal after the expiry of the said period of ninety days, if it is satisfied that the appellant was prevented by sufficient cause from preferring the appeal in time.

Right to legal representation.	76. The applicant or appellant may either appear in person or authorise one or more legal practitioners or any of its officers to present his or its case before the Appellate Tribunal.	
Civil court not to have jurisdiction.	<i>Explanation.—</i> For the purposes of this section, "legal practitioner" includes an advocate, or an attorney and includes a pleader in practice.	5
Grants by Central Government.	77. No civil court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which the Appellate Tribunal is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.	
Data Protection Authority of India Funds.	CHAPTER XII	10
	FINANCE, ACCOUNTS AND AUDIT	
	78. The Central Government may, after due appropriation made by Parliament by law in this behalf, make to the Authority grants of such sums of money as it may think fit for the purposes of this Act.	
Accounts and Audit.	79. (1) There shall be constituted a Fund to be called the Data Protection Authority Fund to which the following shall be credited—	15
	(a) all Government grants, fees and charges received by the Authority under this Act; and	
	(b) all sums received by the Authority from such other source as may be decided upon by the Central Government.	20
	(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 and for the purposes of this Act.	25
Furnishing of returns, etc., to Central Government.	80. (1) The Authority shall maintain proper accounts and other relevant records and prepare an annual statement of accounts in such form as may be prescribed in consultation with the Comptroller and Auditor-General of India.	
	(2) The accounts of the Authority shall be audited by the Comptroller and Auditor-General of India at such intervals as may be prescribed and any expenditure incurred by him in connection with such audit shall be reimbursed to him by the Authority.	30
	(3) The Comptroller and Auditor-General of India and any other person appointed by him in connection with the audit of the accounts of the Authority shall have the same rights and privileges and authority in connection with such audit as the Comptroller and Auditor-General of India generally has in connection with the audit of the Government accounts and, in particular, shall have the right to demand the production of books, accounts, connected vouchers and other documents and papers, and to inspect any of the offices of the Authority.	35
	(4) The accounts of the Authority as certified by the Comptroller and Auditor-General of India or any other person appointed by the Comptroller and Auditor-General of India in this behalf together with the audit report thereon shall be forwarded annually to the Central Government and the Central Government shall cause the same to be laid before each House of the Parliament.	40
	81. (1) The Authority shall furnish to the Central Government at such time and in such form and manner as may be prescribed or as the Central Government may direct, such returns and statements (including statement on enforcement action taken) and such particulars in regard to any proposed or existing programme for the promotion and development of protection of personal data, as the Central Government from time to time, require.	45

(2) The Authority shall prepare once every year in such form and at such time as may be prescribed, an annual report giving a summary of its activities during the previous year and copies of the report shall be forwarded to the Central Government.

5 (3) A copy of the report prepared under sub-section (2) shall be laid, as soon as may be after it is received, before each House of the Parliament.

(4) A copy of the report prepared under sub-section (2) shall also be made publicly available by the Authority.

CHAPTER XIII

OFFENCES

10 **82. (1)** Any person who, knowingly or intentionally—

Re-
identification
and processing
of de-
identified
personal data.

(a) re-identifies personal data which has been de-identified by a data fiduciary or a data processor, as the case may be; or

15 (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.

(2) Nothing contained in sub-section (1) shall render any such person liable to any punishment under this section, if he proves that—

20 (a) the personal data belongs to the person charged with the offence under sub-section (1); or

(b) the data principal whose personal data is in question has explicitly consented to such re-identification or processing as per the provisions of this Act.

2 of 1974. **83. (1)** Notwithstanding anything contained in the Code of Criminal Procedure, 1973, an offence punishable under this Act shall be cognizable and non-bailable.

Offences to
be cognizable
and non-
bailable.

25 (2) No court shall take cognizance of any offence under this Act, save on a complaint made by the Authority.

84. (1) Where an offence under this Act has been committed by a company, every person who, at the time the offence was committed was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company, shall 30 be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

Offences by
companies.

(2) Nothing contained in sub-section (1) shall render any such person liable to any punishment provided in this Act, if he proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such 35 offence.

(3) Notwithstanding anything contained in sub-section (1), where an offence under this Act has been committed by a company and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, 40 secretary or other officer shall also be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

*Explanation.—*For the purpose of this section—

(a) "company" means any body corporate, and includes—

(i) a firm; and

(ii) an association of persons or a body of individuals whether incorporated or not.

(b) "director" in relation to—

(i) a firm, means a partner in the firm;

(ii) an association of persons or a body of individuals, means any member controlling affairs thereof. 5

Offences by State.

85. (1) Where it has been proved that an offence under this Act has been committed by any department or authority or body of the State, by whatever name called, the head of such department or authority or body shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly. 10

(2) Nothing contained in sub-section (1) shall render any such person liable to any punishment provided in this Act, if he proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence.

(3) Notwithstanding anything contained in sub-section (1), where an offence under this Act has been committed by a department of the Central or State Government, or any authority of the State and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any neglect on the part of, any officer, other than the head of the department or authority, such officer shall also be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly. 15 20

(4) Notwithstanding anything in this section, the provisions of the Code of Criminal Procedure, 1973 relating to public servants shall continue to apply.

2 of 1974.

CHAPTER XIV

MISCELLANEOUS

Power of Central Government to issue directions.

86. (1) The Central Government may, from time to time, issue to the Authority such directions as it may think necessary in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order. 25

(2) Without prejudice to the foregoing provisions of this Act, the Authority shall, in exercise of its powers or the performance of its functions under this Act, be bound by such directions on questions of policy as the Central Government may give in writing to it from time to time: 30

Provided that the Authority shall, as far as practicable, be given an opportunity to express its views before any direction is given under this sub-section.

(3) The decision of the Central Government whether a question is one of policy or not shall be final. 35

Members, etc., to be public servants.

87. The Chairperson, Members, officers and employees of the Authority and the Appellate Tribunal shall be deemed, when acting or purporting to act in pursuance of any of the provisions of this Act, to be public servants within the meaning of section 21 of the Indian Penal Code. 45 of 1860.

Protection of action taken in good faith.

88. No suit, prosecution or other legal proceedings shall lie against the Authority or its Chairperson, member, employee or officer for anything which is done in good faith or intended to be done under this Act, or the rules prescribed, or the regulations specified thereunder. 40

Exemption from tax on income.

89. Notwithstanding anything contained in the Income Tax Act, 1961 or any other enactment for the time being in force relating to tax on income, profits or gains, as the case may be, the Authority shall not be liable to pay income tax or any other tax in respect of its income, profits or gains derived. 43 of 1961. 45

90. The Authority may, by general or special order in writing delegate to any member or officer of the Authority subject to such conditions, if any, as may be specified in the order, such of its powers and functions under this Act, except the powers under section 94, as it may deem necessary.

Delegation.

5 **91.** (1) Nothing in this Act shall prevent the Central Government from framing of any policy for the digital economy, including measures for its growth, security, integrity, prevention of misuse, insofar as such policy do not govern personal data.

Act to promote framing of policies for digital economy, etc..

10 (2) The Central Government may, in consultation with the Authority, direct any data fiduciary or data processor to provide any personal data anonymised or other 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.

Explanation.—For the purposes of this sub-section, the expression "non-personal data" means the data other than personal data.

15 (3) The Central Government shall disclose annually the directions, made by it under sub-section (2), in such form as may be prescribed.

92. No data fiduciary shall process such biometric data as may be notified by the Central Government, unless such processing is permitted by law.

Bar on processing certain forms of biometric data.

Power to make rules.

93. (1) The Central Government may, by notification, make rules to carry out the provisions of this Act.

20 (2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:—

(a) any other categories of sensitive personal data under section 15;

(b) other factors to be taken into consideration under clause (d) of sub-section (3) of section 16;

25 (c) the form and manner in which an application may be made to exercise the right under sub-section (2), and the manner of review of the order passed by the Adjudicating Officer under sub-section (4) of section 20;

30 (d) the methods of voluntary identification to identify users of social media under sub-section (3) and the identifying mark of verification of a voluntarily verified user under sub-section (4) of section 28;

(e) the manner in which a complaint may be filed under sub-section (4) of section 32;

(f) the entity or class of entity in a country, or international organisations to which transfers may be permitted under clause (b) of sub-section (1) of section 34;

35 (g) the place of head office of the Authority under sub-section (3) of section 41;

(h) procedure to be followed by the selection committee under sub-section (3) of section 42;

40 (i) the salaries and allowances payable to, and other terms and conditions of service of the Chairperson and the Members of the Authority under sub-section (2) of section 43;

(j) the time and place for, and the rules and procedures in regard to, transaction of business at the meetings of the Authority under sub-section (1) of section 46;

(k) other functions of the Authority under clause (o) of sub-section (2) of section 49;

	(l) the procedure of issuance of a code of practice under sub-section (4), the manner in which the Authority may review, modify or revoke a code of practice under sub-section (7), of section 50;	
	(m) other matters under clause (e) of sub-section (8) of section 53, in respect of which the Authority shall have powers;	5
	(n) the number of Adjudicating Officers, manner and terms of their appointment, their jurisdiction and other requirements under sub-section (2) of section 62;	
	(o) the manner in which the Adjudicating Officer shall conduct an inquiry under sub-section (1) of section 63;	
	(p) the form and manner of making a complaint under sub-section (2), and the procedure for hearing of a complaint under sub-section (8) of section 64;	10
	(q) the manner of appointment, term of office, salaries and allowances, resignation, removal and the other terms and conditions of service of the Chairperson and any member of the Appellate Tribunal under sub-section (2) of section 68;	
	(r) the procedure of filling of vacancies in the Appellate Tribunal under section 69;	15
	(s) the salaries and allowances and other conditions of service of the officers and employees of the Appellate Tribunal under sub-section (3) of section 70;	
	(t) the form, manner and fee for filing an appeal or application, as the case may be, with the Appellate Tribunal under sub-section (1) of section 72;	
	(u) other matters under clause (i) of sub-section (2) of section 73 in respect of powers of the Appellate Tribunal;	20
	(v) the form of accounts, other relevant records and annual statement of accounts under sub-section (1), the intervals at which the accounts of the Authority shall be audited under sub-section (2) of section 80;	
	(w) the time in which and the form and manner in which the returns, statements, and particulars are to be furnished to the Central Government under sub-section (1), and annual report under sub-section (2) of section 81;	25
	(x) the manner in which the Central Government may issue a direction, including the specific purposes for which data is sought under sub-section (2) and the form of disclosure of such directions under sub-section (3) of section 91; or	30
	(y) any other matter which is required to be, or may be, prescribed, or in respect of which provision is to be made, by rules.	
Power to make regulations.	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, namely:—	35
	(a) information required to be provided by the data fiduciary to the data principal in its notice under clause (n) of sub-section (1) of section 7;	
	(b) manner in which the personal data retained by the data fiduciary must be deleted under sub-section (4) of section 9;	40
	(c) the safeguards for protecting the rights of data principals under sub-section (3) of section 14;	
	(d) the additional safeguards or restrictions under sub-section (2) of section 15;	
	(e) the manner of obtaining consent of the parent or guardian of a child under sub-section (2), the manner of verification of age of a child under sub-section (3),	45

application of provision in modified form to data fiduciaries offering counselling or child protection services under sub-section (6) of section 16;

5 (f) the period within which a data fiduciary must acknowledge the receipt of request under sub-section (1), the fee to be charged under sub-section (2), the period within which request is to be complied with under sub-section (3), and the manner and the period within which a data principal may file a complaint under sub-section (4) of section 21;

10 (g) the manner for submission of privacy by design policy under sub-section (2) of section 22;

(h) the manner and the technical, operation, financial and other conditions for registration of the consent manager and its compliance under sub-section (5) of section 23;

(i) the manner of registration of significant data fiduciaries under sub-section (2) of section 26;

15 (j) the circumstances or classes of data fiduciaries or processing operations where data protection impact assessments shall be mandatory and instances where data auditor shall be appointed under sub-section (2), and the manner in which data protection officer shall review the data protection impact assessment and submit to the Authority under sub-section (4) of section 27;

20 (k) the form and manner for maintaining the records, and any other aspect of processing for which records shall be maintained under sub-section (1) of section 28;

(l) the other factors to be taken into consideration under clause (g) of sub-section (2); the form and procedure for conducting audits under sub-section (3); the manner of registration of auditors under sub-section (4); criteria on the basis of which rating in the form of a data trust score may be assigned to a data fiduciary under sub-section (6) of section 29;

(m) the qualification and experience of a data protection officer under sub-section (1) of section 30;

30 (n) the period within which transfer of personal data shall be notified to the Authority under sub-section (3) of section 34;

(o) the provisions of the Act and the class of research, archival or statistical purposes which may be exempted under section 38;

35 (p) the remuneration, salary or allowances and other terms and conditions of service of such officers, employees, consultants and experts under sub-section (2) of section 48;

(q) the code of practice under sub-section (1) of section 50;

(r) the form and manner for providing information to the Authority by the data fiduciary under sub-section (3) of section 52;

40 (s) any other matter which is required to be, or may be specified, or in respect of which provision is to be or may be made by regulations.

95. Every rule and regulation made under this Act and notification issued under sub-section (4) of section 67 shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session

Rules and regulations to be laid before Parliament.

45 immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or regulation or notification or both Houses agree that the rule or regulation or notification should not be made, the rule or regulation or notification shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule or regulation or notification.

Overriding effect of this Act.

Power to remove difficulties.

Amendment of Act 21 of 2000.

Omission of section 43A.

Amendment of section 87.

96. Save as otherwise provided in this Act, the provisions of this Act shall have effect notwithstanding anything inconsistent therewith any other law for the time being in force or any instrument having effect by virtue of any law other than this Act.

97. (1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order, published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to be necessary or expedient for removing the difficulty:

Provided that no such order shall be made under this section after the expiry of five years from the commencement of this Act.

(2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

98. The Information Technology Act, 2000 shall be amended in the manner specified in the Schedule to this Act.

THE SCHEDULE

(See section 98)

5

15

AMENDMENTS TO THE INFORMATION TECHNOLOGY ACT, 2000 (21 OF 2000)

1. Section 43A of the Information Technology Act, 2000 (hereafter in this Schedule referred to as the principal Act) shall be omitted.

2. In section 87 of the principal Act, in sub-section (2), clause (ob) shall be omitted.

20

STATEMENT OF OBJECTS AND REASONS

In the matter of Justice K.S. Puttaswami and another Vs. Union of India [WP 494 of 2012], a nine Judge Constitutional Bench of the Supreme Court, while delivering its judgment on 24th August, 2017, declared "privacy" as a fundamental right under article 21 of the Constitution. Subsequently, on 26th September, 2018, a five Judge Constitutional Bench of the Supreme Court while delivering its final judgment in the above case impressed upon the Government to bring out a robust data protection regime.

2. The Government on 31st July, 2017 constituted a "Committee of Experts on Data Protection" chaired by Justice B.N. Srikrishna to examine the issues relating to data protection. The said Committee examined the issues on data protection and submitted its Report on 27th July, 2018. On the basis of the recommendations made in the said Report and the suggestions received from various stakeholders, it is proposed to enact a legislation, namely, the Personal Data Protection Bill, 2019.

3. The proposed Legislation seeks 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".

4. The salient features of the Data Protection Bill, 2019, *inter alia*, are as under—

(i) to promote the concepts such as consent framework, purpose limitation, storage limitation and the data minimisation;

(ii) to lay down obligations on entities collecting personal data (data fiduciary) to collect only that data which is required for a specific purpose and with the express consent of the individual (data principal);

(iii) to confer rights on the individual to obtain personal data, correct inaccurate data, erase data, update the data, port the data to other fiduciaries and the right to restrict or prevent the disclosure of personal data;

(iv) to establish an Authority to be called the "Data Protection Authority of India" (the Authority) which shall consist of a Chairperson and not more than six whole-time Members to be appointed by the Central Government;

(v) to provide that the Authority shall protect the interests of data principals, prevent any misuse of personal data, ensure compliance with the provisions of the proposed legislation and promote awareness about the data protection;

(vi) to specify a provision relating to "social media intermediary" whose actions have significant impact on electoral democracy, security of the State, public order or the sovereignty and integrity of India and to empower the Central Government, in consultation with the Authority, to notify the said intermediary as a significant data fiduciary;

(vii) to confer a "right of grievance" on data principal to make a complaint against the grievance to the data fiduciary and if aggrieved by the decision of such data fiduciary, he may approach the Authority;

(viii) to empower the Central Government to exempt any agency of Government from application of the proposed Legislation;

(ix) to empower the Authority to specify the "code of practice" to promote good practices of data protection and facilitate compliance with the obligations under this legislation;

(x) to appoint the "Adjudicating Officer" for the purpose of adjudging the penalties to be imposed and the compensation to be awarded under the provisions of this legislation;

(xi) to establish an "Appellate Tribunal" to hear and dispose of any appeal from an order of the Authority under clause 54 and the Adjudicating Officer under clauses 63 and 64; and

(xii) to impose "fines and penalties" for contravention of the provisions of the proposed legislation.

5. The Notes on Clauses explain in detail the various provisions contained in the Bill.

6. The Bill seeks to achieve the above objectives.

NEW DELHI;
The 5th December, 2019.

RAVI SHANKAR PRASAD.

Notes on Clauses

Clause 1.—This clause seeks to provide for short title and commencement of the Act.

Clause 2.—This clause seeks to clarify the application of the Act with regard to personal data of Indians and save for clause 91 would not be applicable to processing of anonymised data.

Clause 3.— This clause seeks to define certain expressions occurring in the Act.

Clause 4.—This clause seeks to prohibit processing of personal data without any specific, clear and lawful purpose.

Clause 5.—This clause seeks to limit the processing of personal data to the purpose consented to by the data principal or which is incidental or connected thereto.

Clause 6.—This clause seeks to lay down limitation on collection of personal data specifying that it should be only to the extent that is necessary.

Clause 7.—This clause seeks to lay down the requirement of notice for collection or processing of personal data and lists the various types of information that should be contained in the notice given to the data principal.

Clause 8.—This clause seeks to lay down that the data fiduciary should ensure the quality of the personal data processed.

Clause 9.—This clause seeks to lay down restriction on retention of personal data beyond what is necessary.

Clause 10.—This clause seeks to lay down the responsibility for complying with the provisions of this Act on the data fiduciary.

Clause 11.—This clause seeks to expound the various aspects of consent which are necessary for processing of personal data.

Clause 12.—This clause seeks to list out certain cases which provide for processing of personal data without consent.

Clause 13.—This clause seeks to provide for processing of personal data necessary for purposes related to employment.

Clause 14.—This clause seeks to provide for other reasonable purposes for which personal data may be processed.

Clause 15.—This clause seeks to provide for categorisation of personal data as sensitive personal data and lists out criteria for such categorisation.

Clause 16.—This clause seeks to provide for obligations on data fiduciaries who processed personal data of children.

Clause 17.—This clause seeks to provide the data principal with the right to confirmation and access to his personal data.

Clause 18.—This clause seeks to provide the data principal with a right to correct and erase his personal data.

Clause 19.—This clause seeks to provide the data principal the right to port personal data to any data fiduciary.

Clause 20.—This clause seeks to provide the data principal the right to be forgotten.

Clause 21.—This clause seeks to lay down the general conditions for the exercise of the rights in clauses 17 to 20.

Clause 22.—This clause seeks to list out the constituents of privacy by design policy.

Clause 23.—This clause seeks to require transparency in processing of personal data by requiring the fiduciary to inform the data principal and making information available.

Clause 24.—This clause seeks to require the data fiduciary to implement necessary security safeguards.

Clause 25.—This clause seeks to require the data fiduciary to report to the Authority about breach of any personal data.

Clause 26.—This clause seeks to provide for classification of certain data fiduciaries as significant data fiduciaries including certain social media intermediaries.

Clause 27.—This clause seeks to require significant data fiduciaries to undertake data protection impact assessment.

Clause 28.—This clause seeks to require significant data fiduciaries to maintain accurate and up-to-date records, including requiring significant social media intermediaries to provide for voluntary verification mechanism.

Clause 29.—This clause seeks to require significant data fiduciaries to have their policies and conduct audited by data auditors.

Clause 30.—This clause seeks to require significant data fiduciaries to appoint a Data Protection Officer.

Clause 31.—This clause seeks to require data fiduciaries to ensure a contract for processing by other data processors.

Clause 32.—This clause seeks to require every data fiduciary to have a grievance redressal mechanism.

Clause 33.—This clause seeks to prohibit processing of sensitive personal data and critical personal data outside India.

Clause 34.—This clause seeks to list out conditions under which sensitive personal data and critical personal data could be transferred outside India.

Clause 35.—This clause seeks to empower the Central Government to exempt any agency of the Government from application of the Act.

Clause 36.—This clause seeks to provide for exemption of certain provisions of the Act for certain processing of personal data.

Clause 37.—This clause seeks to clarify that the Government could exempt certain data processors who are processing data of foreigners, from the application of this Act.

Clause 38.—This clause seeks to provide for exemption when personal data is processed for research, archival or statistical purposes.

Clause 39.—This clause seeks to provide for exemption for small entities who are engaged in manual processing of personal data.

Clause 40.—This clause seeks to provide for a Sandbox which can facilitate new ideas and approaches without any regulatory violations.

Clause 41.—This clause seeks to establish a regulator namely the Data Protection Authority of India (the Authority).

Clause 42—This clause seeks to lift the compositions and qualifications for appointment of Chairperson and Members of the Authority and their method of selection.

Clause 43.—This clause seeks to list the terms and conditions of appointment for the Chairperson and Members of the Authority.

Clause 44.—This clause seeks to list the conditions under which a Chairperson or other Members of the Authority can be removed.

Clause 45.—This clause seeks to lay down that the powers of the Authority rests with the Chairperson

Clause 46.—This clause seeks to provide for the matters relating to meetings of the Authority.

Clause 47.—This clause seeks to provide that the proceedings of the Authority would not be invalidated due to vacancy, procedural irregularity, etc.

Clause 48.—This clause seeks to empower the Authority to appoint officers and other employees.

Clause 49.—This clause seeks to list the powers and functions of the Authority.

Clause 50.—This clause seeks to require the Authority to specify codes of practice to promote good practices of data protection.

Clause 51.—This clause seeks to empower the Authority to issue directions to any data fiduciary for the discharge of its functions.

Clause 52.—This clause seeks to empower the Authority to call for information from any data fiduciary

Clause 53.—This clause seeks to empower the Authority to conduct an inquiry into the affairs of a data fiduciary.

Clause 54.—This clause seeks to list out various actions that can be taken by the Authority pursuant to an inquiry

Clause 55.—This clause seeks to empower the Inquiry Officer of the Authority to order for search and seizure of documents, records, etc.

Clause 56.—This clause seeks to provide for coordination between the Authority and other regulators.

Clause 57.—This clause seeks to list out penalties for contravening certain provisions of the Act.

Clause 58.—This clause seeks to list out penalties for failure to comply with request made by data principal.

Clause 59.—This clause seeks to list out penalty for failure of the data fiduciary to furnish report, return, information to the Authority.

Clause 60.—This clause seeks to list out penalty for failure of the data fiduciary to comply with direction or order issued by the Authority.

Clause 61.—This clause seeks to list out penalty for contravention of any provision of this Act or rules or regulations made thereunder for which no separate penalty has been provided.

Clause 62.—This clause seeks to provide for appointment of Adjudicating Officer for adjudging penalties.

Clause 63.—This clause seeks to lay down the procedure for adjudication by Adjudicating Officer.

Clause 64.—This clause seeks to provide for data principal's right to seek compensation from the data fiduciary in case of suffering harm.

Clause 65.—This clause seeks to ensure that compensation or penalties under this Act would not interfere with any other penalty or punishment.

Clause 66.—This clause seeks to lay down that penalties or compensation awarded under this Act may be recovered as arrear of land revenue.

Clause 67.—This clause seeks to lay down provisions relating to establishment of Appellate Tribunal.

Clause 68.—This clause seeks to list out qualifications, appointment, term, conditions of service of Chairperson and Members of Appellate Tribunal.

Clause 69.—This clause seeks to provide for filling up vacancies in the office of Chairperson and Members of Appellate Tribunal.

Clause 70.—This clause seeks to provide for staffing of Appellate Tribunal.

Clause 71.—This clause seeks to provide for distribution of business to different benches of the Appellate Tribunal.

Clause 72.—This clause seeks to provide for appeal to the Appellate Tribunal against any decision of the Authority.

Clause 73.—This clause seeks to lay down the procedure and powers of the Appellate Tribunal.

Clause 74.—This clause seeks to provide that the Appellate Tribunal shall have all the powers of a civil court.

Clause 75.—This clause seeks to provide for an appeal to the Supreme Court against any order of the Appellate Tribunal.

Clause 76.—This clause seeks to provide for the applicant or appellant to appear in person or authorise legal representative.

Clause 77.—This clause seeks to lay down that no civil court would have jurisdiction to entertain any suit on any matter which falls within the ambit of Appellate Tribunal.

Clause 78.—This clause seeks to provide for the Central Government to make grants to the Authority.

Clause 79.—This clause seeks to provide for constitution of the Data Protection Authority Fund.

Clause 80.—This clause seeks to require the Authority to maintain proper accounts which are to be audited by the Comptroller and Auditor-General of India.

Clause 81.—This clause seeks to require the Authority to furnish returns, statements, etc., to the Central Government.

Clause 82.—This clause seeks to list out punishment for the offence of reidentifying of deidentified personal data.

Clause 83.—This clause seeks to lays out that offence in Clause 82 to be cognizable and non-bailable.

Clause 84.—This clause seeks to list out provisions relating to commission of offence by companies.

Clause 85.—This clause seeks to list out provisions relating to commission of offence by any State Government or Central Government Department or agency.

Clause 86.—This clause seeks to empower the Central Government to issue directions to the Authority.

Clause 87.—This clause seeks to deem Members, officers etc. of the Authority to be public servants when acting pursuant to any provisions of the Act.

Clause 88.—This clause seeks to protect the Authority, Member, employee in case of action done under this Act in good faith.

Clause 89.—This clause seeks to exempts Authority from tax on income in respect of its income, profits.

Clause 90.—This clause seeks to empower the Authority to delegate its powers or functions to any Member or officer.

Clause 91.—This clause seeks to empower the Central Government to frame policies for digital economy in respect of non-personal data.

Clause 92.—This clause seeks to ban processing of certain forms of biometric data unless permitted by law.

Clause 93.—This clause seeks to empowers the Central Government to make rules to carry out the provisions of the Act.

Clause 94.—This clause seeks to empowers the Authority to make regulations consistent with the Act and rules made there under.

Clause 95.—This clause seeks to require that rules and regulations made under this Act are to be laid before the Parliament.

Clause 96.—This clause seeks to provide for the overriding effect of this Act notwithstanding anything inconsistent with any other law.

Clause 97.—This clause seeks to provide for power of Central Government to remove difficulties.

Clause 98.—This clause seeks to provide for related amendments to the Informations Technology Act, 2000.

FINANCIAL MEMORANDUM

Sub-clause (2) of clause 43 provides for the payment of salaries and allowances to the Chairperson, Members of the Authority.

2. Sub-clause (2) of clause 48 provides for the payment of salaries and allowances to the officers and employees of the Authority.

3. Sub-clause (2) of clause 68 provides for the payment of salaries and allowances to the Chairperson and Members of the Appellate Tribunal.

4. Sub-clause (3) of clause 70 provides for the payment of salaries and allowances to the officers and employees of the Appellate Tribunal.

5. For the aforesaid provisions, it would involve an expenditure of (recurring or non-recurring) one hundred crore rupees from the Consolidated Fund of India.

MEMORANDUM REGARDING DELEGATED LEGISLATION

Clause 93 of the Personal Data Protection Bill 2019 seeks to empower the Central Government to make rules for—(a) categorization of sensitive personal data under section 15; (b) verification of the age of child under sub-section (3) of section (3); (c) the form and manner in which an application to enforce the right to be forgotten can be exercised under sub-section (2) of section 20 and the manner of review of order passed by the Adjudicating Officer under sub-section (4) of section 20; (d) the methods of voluntary identification to identify users of social media under sub-section (3) and the identifying mark of verification of a voluntarily verified user under sub-section (4) of section 28; (e) the manner in which a complaint regarding grievance redressal may be filed under sub-section (4) of section 32 ; (f) the entity or class of entity in a country, or international organisations to which transfers may be permitted under clause (b) of sub-section (1) of section 34; (g) the place of head office of the Authority under sub-section (3) of section 41; (h) procedure to be followed by the Selection Committee under sub-section (3) of section 42; (i) the salaries and allowances payable to, and other terms and conditions of service of the Chairperson and the Members of the Authority under sub-section (2) of section 43; (j) the procedure for conducting any inquiry under sub-section (2) of section 44; (k) the time and place for, and the rules and procedures in regard to, transaction of business at the meetings of the Authority under sub-section (1) of section 46; (l) other functions of the Authority under clause (o) of sub-section (2) of section 49; (m) the procedure of issuance of a code of practice under sub-section (4), the manner in which the Authority may review, modify or revoke a code of practice under sub-section (7), of section 50; (n) other matters under clause (e) of sub-section (8) of section 53 in respect of which the Authority shall have powers; (o) the number of Adjudicating Officers, manner and terms of their appointment, their jurisdiction and other requirements under sub-section (2) of section 62; (p) the manner in which the Adjudicating Officer shall conduct an inquiry under sub-section (1) of section 63; (q) the form and manner of making a complaint under sub-section (2), and the procedure for hearing of a complaint under sub-section (8) of section 64; (r) the manner of appointment, term of office, salaries and allowances, resignation, removal and the other terms and conditions of service of the Chairperson and any member of the Appellate Tribunal under sub-section (2) of section 68; (s) the procedure of filling of vacancies in the Appellate Tribunal under section 69; (t) the salaries and allowances and other conditions of service of the officers and employees of the Appellate Tribunal under sub-section (3) of section 70; (u) the form, manner and fee for filing an appeal or application, as the case may be, with the Appellate Tribunal under sub-section (1) of section 72; (v) other matters under clause (i) of sub-section (2) of section 73 in respect of powers of the Appellate Tribunal; (w) the form of accounts, other relevant records and annual statement of accounts under sub-section (1), the intervals at which the accounts of the Authority shall be audited under sub-section (2) of section 80; (x) the time in which and the form and manner in which the returns, statements, and particulars are to be furnished to the Central Government under sub-section (1) and annual report under sub-section (2) of section 81; (y) the manner in which the Central Government may issue a direction, including the specific purposes for which data is sought under sub-section (2) and the form of disclosure of such directions under sub-section (3) of section 91; (z) any other matter which is required to be, or may be, prescribed, or in respect of which provision is to be made, by rules.

2. Clause 94 of the Bill empowers the Authority, with the previous approval of the Central Government, by notification, to make regulations consistent with the provisions of the Act and the rules made thereunder to provide for—(a) information required to be provided by the data fiduciary to the data principal in its notice under clause (n) of sub-section (1) of section 7; (b) manner in which the personal data retained by the data fiduciary must be deleted under sub-section (4) of section 9; (c) the safeguards for protecting the rights of data

principals under sub-section (3) of section 14; (d) the additional safeguards or restrictions under sub-section (2) of section 15; (e) the manner of obtaining consent of the parent or guardian of a child under sub-section (2), the manner of verification of age of a child under sub-section (3), application of provision in modified form to data fiduciaries offering counselling or child protection services under sub-section (6) of section 16; (f) the period within which a data fiduciary must acknowledge the receipt of request under sub-section (1), the fee to be charged under sub-section (2), the period within which request is to be complied with under sub-section (3), and the manner and the period within which a data principal may file a complaint under sub-section (4) of section 21; (g) the manner for submission of privacy by design policy under sub-section (2) of section 22; (h) the manner and the technical, operation, financial and other conditions for registration of the consent manager and its compliance under sub-section (5) of section 23; (i) the manner of registration of significant data fiduciaries under sub-section (2) of section 26; (j) the circumstances or classes of data fiduciaries or processing operations where data protection impact assessments shall be mandatory and instances where data auditor shall be appointed under sub-section (2), and the manner in which data protection officer shall review the data protection impact assessment and submit to the Authority under sub-section (4) of section 27; (k) the form and manner for maintaining the records, and any other aspect of processing for which records shall be maintained under sub-section (1) of section 28; (l) the other factors to be taken into consideration under clause (g) of sub-section (2); the form and procedure for conducting audits under sub-section (3); the manner of registration of auditors under sub-section (4); criteria on the basis of which rating in the form of a data trust score may be assigned to a data fiduciary under sub-section (6) of section 29; (m) the qualification and experience of a data protection officer under sub-section (1) of section 30; (n) the period within which transfer of personal data shall be notified to the Authority under sub-section (3) of section 34; (o) the provisions of the Act and the class of research, archival or statistical purposes which may be exempted under section 38; (p) the remuneration, salary or allowances and other terms and conditions of service of such officers, employees, consultants and experts under sub-section (2) of section 48; (q) the code of practice under sub-section (1) of section 50; (r) the form and manner for providing information to the Authority by the data fiduciary under sub-section (3) of section 52; and (s) any other matter which is required to be, or may be specified, or in respect of which provision is to be or may be made by regulations.

3. The matters in respect of which the aforementioned rules and regulations may be made are matters of procedure and administrative detail, and as such, it is not practicable to provide for them in the proposed Bill itself. The delegation of legislative power is, therefore, of a normal character.

ANNEXURE

EXTRACTS FROM THE INFORMATION TECHNOLOGY ACT, 2000 (21 OF 2000)

* * * * *

43A. Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Compensation
for failure to
protect data.

Explanation.—For the purposes of this section,—

(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

* * * * *

87. (I) * * * * *

Power of
Central
Government
to make rules.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:—

* * * * *

(ob) the reasonable security practices and procedures and sensitive personal data or information under section 43A;

* * * * *

LOK SABHA

A

BILL

to provide for protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the rights of individuals whose personal data are processed, to create a framework for organisational and technical measures in processing of data, laying down norms for social media intermediary, cross-border transfer, accountability of entities processing personal data, remedies for unauthorised and harmful processing, and to establish a Data Protection Authority of India for the said purposes and for matters connected therewith or incidental thereto.

(Shri Ravi Shankar Prasad, Minister of Law and Justice, Communications and Electronics and Information Technology)

THE PERSONAL DATA PROTECTION BILL, 2018

CHAPTER I

PRELIMINARY

1.	Short title, extent and commencement.—	1
2.	Application of the Act to processing of personal data.—	1
3.	Definitions.— In this Act, unless the context otherwise requires, —.....	2

CHAPTER II

DATA PROTECTION OBLIGATIONS

4.	Fair and reasonable processing.—	6
5.	Purpose limitation.—	6
6.	Collection limitation. —	7
7.	Lawful processing.—	7
8.	Notice.—	7
9.	Data quality.—	8
10.	Data storage limitation.—	8
11.	Accountability.—	9

CHAPTER III

GROUNDS FOR PROCESSING OF PERSONAL DATA

12.	Processing of personal data on the basis of consent.—	9
13.	Processing of personal data for functions of the State. —	10
14.	Processing of personal data in compliance with law or any order of any court or tribunal. — 10	
15.	Processing of personal data necessary for prompt action. —	10
16.	Processing of personal data necessary for purposes related to employment. —.....	10
17.	Processing of data for reasonable purposes. —.....	11

CHAPTER IV

GROUNDS FOR PROCESSING OF SENSITIVE PERSONAL DATA

18.	Processing of sensitive personal data based on explicit consent. —.....	11
19.	Processing of sensitive personal data for certain functions of the State. —	12
20.	Processing of sensitive personal data in compliance with law or any order of any court or tribunal. —	12
21.	Processing of certain categories of sensitive personal data for prompt action. —.....	12

22. Further categories of sensitive personal data.—	13
---	----

CHAPTER V

PERSONAL AND SENSITIVE PERSONAL DATA OF CHILDREN

23. Processing of personal data and sensitive personal data of children. —.....	13
---	----

CHAPTER VI

DATA PRINCIPAL RIGHTS

24. Right to confirmation and access. —	14
25. Right to correction, etc.—	14
26. Right to Data Portability. —	15
27. Right to Be Forgotten. —.....	16
28. General conditions for the exercise of rights in this Chapter. —.....	16

CHAPTER VII

TRANSPARENCY AND ACCOUNTABILITY MEASURES

29. Privacy by Design. —	17
30. Transparency. —	18
31. Security Safeguards.—	18
32. Personal Data Breach.—	18
33. Data Protection Impact Assessment. —.....	19
34. Record-Keeping. —	20
35. Data Audits. —.....	20
36. Data Protection Officer. —	21
37. Processing by entities other than data fiduciaries. —	22
38. Classification of data fiduciaries as significant data fiduciaries. —	22
39. Grievance Redressal. —.....	23

CHAPTER VIII

TRANSFER OF PERSONAL DATA OUTSIDE INDIA

40. Restrictions on Cross-Border Transfer of Personal Data. —	23
41. Conditions for Cross-Border Transfer of Personal Data. —.....	24

CHAPTER IX

EXEMPTIONS

42. Security of the State.—	25
43. Prevention, detection, investigation and prosecution of contraventions of law.—.....	25

44.	Processing for the purpose of legal proceedings.—.....	26
45.	Research, archiving or statistical purposes. —	27
46.	Personal or domestic purposes. —	27
47.	Journalistic purposes.—	28
48.	Manual processing by small entities.—	28

CHAPTER X

DATA PROTECTION AUTHORITY OF INDIA

49.	Establishment and incorporation of Authority.—	29
50.	Composition and qualifications for appointment of members.—	29
51.	Terms and conditions of appointment.—	30
52.	Removal of members.—	30
53.	Powers of the chairperson.—	31
54.	Meetings of the Authority.—	31
55.	Vacancies, etc. not to invalidate proceedings of the Authority.—.....	31
56.	Officers and Employees of the Authority.—	31
57.	Grants by Central Government.—	32
58.	Accounts and Audit —	32
59.	Furnishing of returns, etc. to Central Government.—.....	32
60.	Powers and Functions of the Authority.—	33
61.	Codes of Practice.—.....	35
62.	Power of Authority to issue directions.—	36
63.	Power of Authority to call for information.—	37
64.	Power of Authority to conduct inquiry. —	37
65.	Action to be taken by Authority pursuant to an inquiry.—.....	38
66.	Search and Seizure.—	39
67.	Coordination between the Authority and other regulators or authorities.—.....	40
68.	Appointment of Adjudicating Officer.—	41

CHAPTER XI

PENALTIES AND REMEDIES

69.	Penalties.—	41
70.	Penalty for failure to comply with data principal requests under Chapter VI.—.....	42
71.	Penalty for failure to furnish report, returns, information, etc.—	42

72.	Penalty for failure to comply with direction or order issued by the Authority.—	43
73.	Penalty for contravention where no separate penalty has been provided.—	43
74.	Adjudication by Adjudicating Officer.—.....	43
75.	Compensation.—.....	44
76.	Compensation or penalties not to interfere with other punishment.—	45
77.	Data Protection Funds.—	45
78.	Recovery of Amounts.—.....	46

CHAPTER XII

APPELLATE TRIBUNAL

79.	Establishment of Appellate Tribunal.—.....	47
80.	Qualifications, appointment, term, conditions of service of members.—.....	48
81.	Vacancies.—	48
82.	Staff of Appellate Tribunal.—	48
83.	Distribution of business amongst benches.—	48
84.	Appeals to Appellate Tribunal.—	49
85.	Procedure and powers of Appellate Tribunal.—.....	49
86.	Orders passed by Appellate Tribunal to be executable as a decree.—	50
87.	Appeal to Supreme Court of India.—	50
88.	Right to legal representation.—	50
89.	Civil court not to have jurisdiction.—.....	51

CHAPTER XIII

OFFENCES

90.	Obtaining, transferring or selling of personal data contrary to the Act.—.....	51
91.	Obtaining, transferring or selling of sensitive personal data contrary to the Act.—.....	51
92.	Re-identification and processing of de-identified personal data. —.....	52
93.	Offences to be cognizable and non-bailable.—	52
94.	Power to investigate offences.—	52
95.	Offences by companies.—	52
96.	Offences by Central or State Government departments. —.....	53

CHAPTER XIV

TRANSITIONAL PROVISIONS

97.	Transitional provisions and commencement. —.....	54
-----	--	----

CHAPTER XV
MISCELLANEOUS

98. Power of Central Government to issue directions in certain circumstances. —	55
99. Members, etc., to be public servants. —	55
100. Protection of action taken in good faith. —	55
101. Exemption from tax on income. —	55
102. Delegation. —	55
103. Power to remove difficulties. —	56
104. Power to exempt certain data processors.—	56
105. No application to non-personal data.....	56
106. Bar on processing certain forms of biometric data.....	56
107. Power to make rules. —	56
108. Power to make regulations. —	58
109. Rules and Regulations to be laid before Parliament.—.....	59
110. Overriding effect of this Act. —	60
111. Amendment of Act 21 of 2000. —.....	60
112. Amendment of Act 22 of 2005. —.....	60
THE FIRST SCHEDULE	61
THE SECOND SCHEDULE.....	62

THE PERSONAL DATA PROTECTION BILL, 2018

WHEREAS the right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of informational privacy;

WHEREAS the growth of the digital economy has meant the use of data as a critical means of communication between persons;

WHEREAS it is necessary to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress and innovation;

AND WHEREAS it is expedient to make provision: to protect the autonomy of individuals in relation with their personal data, to specify where the flow and usage of personal data is appropriate, to create a relationship of trust between persons and entities processing their personal data, to specify the rights of individuals whose personal data are processed, to create a framework for implementing organisational and technical measures in processing personal data, to lay down norms for cross-border transfer of personal data, to ensure the accountability of entities processing personal data, to provide remedies for unauthorised and harmful processing, and to establish a Data Protection Authority for overseeing processing activities;

BE IT ENACTED by Parliament in the Sixty-Ninth Year of the Republic of India as follows: —

CHAPTER I PRELIMINARY

1. Short title, extent and commencement.—

- (1) This Act may be called the Personal Data Protection Act, 2018.
- (2) It extends to the whole of India.
- (3) The provisions of Chapter XIV of this Act shall come into force on such date, as the Central Government may by notification appoint and the remaining provisions of the Act shall come into force in accordance with the provisions in that Chapter.

2. Application of the Act to processing of personal data.—

- (1) This Act applies to the following—
 - (a) processing of personal data where such data has been collected, disclosed, shared or otherwise processed within the territory of India; and
 - (b) processing of personal data by the State, any Indian company, any Indian citizen or any person or body of persons incorporated or created under Indian law.

- (2) Notwithstanding anything contained in sub-section (1), the Act shall apply to the processing of personal data by data fiduciaries or data processors not present within the territory of India, only if such processing is —
 - (a) in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within the territory of India; or
 - (b) in connection with any activity which involves profiling of data principals within the territory of India.
- (3) Notwithstanding anything contained in sub-sections (1) and (2), the Act shall not apply to processing of anonymised data.

3. Definitions.—In this Act, unless the context otherwise requires,—

- (1) “**Aadhaar number**” shall have the meaning assigned to it under clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016);
- (2) “**Adjudicating Officer**” means an officer of the adjudication wing under section 68;
- (3) “**Anonymisation**” in relation to personal data, means the irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, meeting the standards specified by the Authority.
- (4) “**Anonymised data**” means data which has undergone the process of anonymisation under sub-clause (3) of this section;
- (5) “**Appellate Tribunal**” means the tribunal notified under Chapter XII of this Act;
- (6) “**Authority**” means the Data Protection Authority of India established under Chapter X of this Act;
- (7) “**Automated means**” means any equipment capable of operating automatically in response to instructions given for the purpose of processing data;
- (8) “**Biometric data**” means facial images, fingerprints, iris scans, or any other similar personal data resulting from measurements or technical processing operations carried out on physical, physiological, or behavioural characteristics of a data principal, which allow or confirm the unique identification of that natural person;
- (9) “**Child**” means a data principal below the age of eighteen years;
- (10) “**Code of Practice**” means a code of practice issued by the Authority under section 61;
- (11) “**Consent**” means consent under section 12;

- (12) “**Data**”means and includes a representation of information, facts, concepts, opinions, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automated means;
- (13) “**Data fiduciary**”means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data;
- (14) “**Data principal**”means the natural person to whom the personal data referred to in sub-clause (28) relates;
- (15) “**Data processor**”means any person, including the State, a company, any juristic entity or any individual who processes personal data on behalf of a data fiduciary, but does not include an employee of the data fiduciary;
- (16) “**De-identification**”means the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal;
- (17) “**Disaster**” shall have the same meaning assigned to it under clause (d) of section 2 of the Disaster Management Act, 2005 (53 of 2005);
- (18) “**Explicit consent**”means consent under section 18;
- (19) “**Financial data**”means any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal or any personal data regarding the relationship between a financial institution and a data principal including financial status and credit history;
- (20) “**Genetic data**”means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the behavioural characteristics, physiology or the health of that natural person and which result,in particular, from an analysis of a biological sample from the natural person in question;
- (21) “**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.
- (22) “**Health data**” means data related to the state of physical or mental health of the data principal and includes records regarding the past, present or future state of the health of such data principal, data collected in the course of registration for, or provision of health services, data associating the data principal to the provision of specific health services.
- (23) “**Intersex status**” means the condition of a data principal who is—
- (i) a combination of female or male;
 - (ii) neither wholly female nor wholly male; or
 - (iii) neither female nor male.
- (24) “**Intra-group schemes**” means schemes approved by the Authority under section 41;
- (25) “**Journalistic purpose**” means any activity intended towards the dissemination through print, electronic or any other media of factual reports, analysis, opinions, views or documentaries regarding—
- (i) news, recent or current events; or
 - (ii) any other information which the data fiduciary believes the public, or any significantly discernible class of the public, to have an interest in;
- (26) “**Notification**” means a notification published in the Official Gazette and the term “notify” shall be construed accordingly;
- (27) “**Official identifier**” means any number, code, or other identifier, including Aadhaar number, assigned to a data principal under a law made by Parliament or any State Legislature which may be used for the purpose of verifying the identity of a data principal;
- (28) “**Person**” means—
- (i) an individual,
 - (ii) a Hindu undivided family,
 - (iii) a company,

- (iv) a firm,
 - (v) an association of persons or a body of individuals, whether incorporated or not,
 - (vi) the State, and
 - (vii) every artificial juridical person, not falling within any of the preceding sub-clauses;
- (29) “**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, or any combination of such features, or any combination of such features with any other information;
- (30) “**Personal data breach**” means any unauthorised or accidental disclosure, acquisition, sharing, use, alteration, destruction, loss of access to, of personal data that compromises the confidentiality, integrity or availability of personal data to a data principal;
- (31) “**Prescribed**”means prescribed by rules made by the Central Government under this Act;
- (32) “**Processing**”in relation to personal data, means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;
- (33) “**Profiling**”means any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interest of a data principal;
- (34) “**Re-identification**”means the process by which a data fiduciary or data processor may reverse a process of de-identification;
- (35) “**Sensitive Personal Data**”means personal data revealing, related to, or constituting, as may be applicable—
- (i) passwords;
 - (ii) financial data;
 - (iii) health data;
 - (iv) official identifier;
 - (v) sex life;
 - (vi) sexual orientation;
 - (vii) biometric data;
 - (viii) genetic data;
 - (ix) transgender status;
 - (x) intersex status;
 - (xi) caste or tribe;

- (xii) religious or political belief or affiliation; or
 - (xiii) any other category of data specified by the Authority under section 22.
- (36) “**Significant data fiduciary**” means a data fiduciary notified by the Authority under section 38;
- (37) “**Significant harm**” means harm that has an aggravated effect having regard to the nature of the personal data being processed, the impact, continuity, persistence or irreversibility of the harm;
- (38) “**Specified**” means specified by regulations made by the Authority under this Act and the term “specify” shall be construed accordingly;
- (39) “**State**” shall, unless the context otherwise requires, have the same meaning assigned to it under Article 12 of the Constitution;
- (40) “**Systematic activity**” means any structured or organised activity that involves an element of planning, method, continuity or persistence;
- (41) “**Transgender status**” means the condition of a data principal whose sense of gender does not match with the gender assigned to that data principal at birth, whether or not they have undergone sex reassignment surgery, hormone therapy, laser therapy, or any other similar medical procedure.

CHAPTER II

DATA PROTECTION OBLIGATIONS

4. Fair and reasonable processing.—Any person processing personal data owes a duty to the data principal to process such personal data in a fair and reasonable manner that respects the privacy of the data principal.

5. Purpose limitation.—

- (1) Personal data shall be processed only for purposes that are clear, specific and lawful.
- (2) Personal data shall be processed only for purposes specified or for any other incidental purpose that the data principal would reasonably expect the personal data to be used for, having regard to the specified purposes, and the context and circumstances in which the personal data was collected.

6. **Collection limitation.** —Collection of personal data shall be limited to such data that is necessary for the purposes of processing.

7. Lawful processing.—

- (1) Personal data shall be processed only on the basis of one or a combination of grounds of processing in Chapter III.
- (2) Sensitive personal data shall be processed only on the basis of one or a combination of grounds of processing in Chapter IV.

8. Notice.—

- (1) The data fiduciary shall provide the data principal with the following information, no later than at the time of collection of the personal data or, if the data is not collected from the data principal, as soon as is reasonably practicable—
 - (a) the purposes for which the personal data is to be processed;
 - (b) the categories of personal data being collected;
 - (c) the identity and contact details of the data fiduciary and the contact details of the data protection officer, if applicable;
 - (d) the right of the data principal to withdraw such consent, and the procedure for such withdrawal, if the personal data is intended to be processed on the basis of consent;
 - (e) the basis for such processing, and the consequences of the failure to provide such personal data, if the processing of the personal data is based on the grounds in section 12 to section 17, and section 18 to section 22;
 - (f) the source of such collection, if the personal data is not collected from the data principal;
 - (g) the individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared, if applicable;
 - (h) information regarding any cross-border transfer of the personal data that the data fiduciary intends to carry out, if applicable;
 - (i) the period for which the personal data will be retained in terms of section 10 or where such period is not known, the criteria for determining such period;
 - (j) the existence of and procedure for the exercise of data principal rights mentioned in Chapter VI and any related contact details for the same;
 - (k) the procedure for grievance redressal under section 39;
 - (l) the existence of a right to file complaints to the Authority;
 - (m) where applicable, any rating in the form of a data trust score that may be assigned to the data fiduciary under section 35; and
 - (n) any other information as may be specified by the Authority.

- (2) The data fiduciary shall provide the information as required under this section to the data principal in a clear and concise manner that is easily comprehensible to a reasonable person and in multiple languages where necessary and practicable.
- (3) Sub-section (1) shall not apply where the provision of notice under this section would substantially prejudice the purpose of processing of personal data under sections 15 or 21 of this Act.

9. Data quality.—

- (1) The data fiduciary shall take reasonable steps to ensure that personal data processed is complete, accurate, not misleading and updated, having regard to the purposes for which it is processed.
- (2) In considering whether any reasonable step is necessary under sub-section (1), the data fiduciary shall have regard to whether the personal data—
 - (a) is likely to be used to make a decision about the data principal;
 - (b) is likely to be disclosed to other individuals or entities including other data fiduciaries or processors; or
 - (c) is kept in a form that distinguishes personal data based on facts from personal data based on opinions or personal assessments.
- (3) Where personal data is disclosed to other individuals or entities, including other data fiduciaries or processors, and the data fiduciary subsequently finds that such data does not comply with sub-section (1), the data fiduciary shall take reasonable steps to notify such individuals or entities of this fact.

10. Data storage limitation.—

- (1) The data fiduciary shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed.
- (2) Notwithstanding sub-section (1), personal data may be retained for a longer period of time if such retention is explicitly mandated, or necessary to comply with any obligation, under a law.
- (3) The data fiduciary must undertake periodic review in order to determine whether it is necessary to retain the personal data in its possession.
- (4) Where it is not necessary for personal data to be retained by the data fiduciary under sub-sections (1) and (2), then such personal data must be deleted in a manner as may be specified.

11. Accountability.—

- (1) The data fiduciary shall be responsible for complying with all obligations set out in this Act in respect of any processing undertaken by it or on its behalf.
- (2) The data fiduciary should be able to demonstrate that any processing undertaken by it or on its behalf is in accordance with the provisions of this Act.

CHAPTER III
GROUNDS FOR PROCESSING OF PERSONAL DATA

12. Processing of personal data on the basis of consent.—

- (1) Personal data may be processed on the basis of the consent of the data principal, given no later than at the commencement of the processing.
- (2) For the consent of the data principal to be valid, it must be—
 - (a) free, having regard to whether it meets the standard under section 14 of the Indian Contract Act, 1872 (9 of 1872);
 - (b) informed, having regard to whether the data principal has been provided with the information required under section 8;
 - (c) specific, having regard to whether the data principal can determine the scope of consent in respect of the purposes of processing;
 - (d) clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given context; and
 - (e) capable of being withdrawn, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given.
- (3) The data fiduciary shall not make the provision of any goods or services or the quality thereof, the performance of any contract, or the enjoyment of any legal right or claim, conditional on consent to processing of any personal data not necessary for that purpose.
- (4) The data fiduciary shall bear the burden of proof to establish that consent has been given by the data principal for processing of personal data in accordance with sub-section (2).
- (5) Where the data principal withdraws consent for the processing of any personal data necessary for the performance of a contract to which the data principal is a party, all legal consequences for the effects of such withdrawal shall be borne by the data principal.

13. Processing of personal data for functions of the State. —

- (1) Personal data may be processed if such processing is necessary for any function of Parliament or any State Legislature.
- (2) Personal data may be processed if such processing is necessary for the exercise of any function of the State authorised by law for:
 - (a) the provision of any service or benefit to the data principal from the State; or
 - (b) the issuance of any certification, license or permit for any action or activity of the data principal by the State.

14. Processing of personal data in compliance with law or any order of any court or tribunal. —

Personal data may be processed if such processing is—

- (a) explicitly mandated under any law made by Parliament or any State Legislature; or
- (b) for compliance with any order or judgment of any Court or Tribunal in India.

15. Processing of personal data necessary for prompt action. —

Personal data may be processed if such processing is necessary—

- (a) 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;
- (b) 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; or
- (c) to undertake any measure to ensure safety of, or provide assistance or services to, any individual during any disaster or any breakdown of public order.

16. Processing of personal data necessary for purposes related to employment. —

- (1) Personal data may be processed if such processing is necessary for—
 - (a) recruitment or termination of employment of a data principal by the data fiduciary;
 - (b) provision of any service to, or benefit sought by, the data principal who is an employee of the data fiduciary;
 - (c) verifying the attendance of the data principal who is an employee of the data fiduciary; or
 - (d) any other activity relating to the assessment of the performance of the data principal who is an employee of the data fiduciary.
- (2) Sub-section (1) shall apply only where processing on the basis of consent of the data principal is not appropriate having regard to the employment relationship between the

data fiduciary and the data principal, or would involve a disproportionate effort on the part of the data fiduciary due to the nature of the processing activities under this section.

17. Processing of data for reasonable purposes. —

- (1) In addition to the grounds for processing contained in section 12 to section 16, personal data may be processed if such processing is necessary for such reasonable purposes as may be specified after taking into consideration—
 - (a) the interest of the data fiduciary in processing for that purpose;
 - (b) whether the data fiduciary can reasonably be expected to obtain the consent of the data principal;
 - (c) any public interest in processing for that purpose;
 - (d) the effect of the processing activity on the rights of the data principal; and
 - (e) the reasonable expectations of the data principal having regard to the context of the processing.
- (2) For the purpose of sub-section (1), the Authority may specify reasonable purposes related to the following activities, including—
 - (a) prevention and detection of any unlawful activity including fraud;
 - (b) whistle blowing;
 - (c) mergers and acquisitions;
 - (d) network and information security;
 - (e) credit scoring;
 - (f) recovery of debt;
 - (g) processing of publicly available personal data;
- (3) Where the Authority specifies a reasonable purpose under sub-section (1), it shall:
 - (a) lay down such safeguards as may be appropriate to ensure the protection of the rights of data principals; and
 - (b) determine where the provision of notice under section 8 would not apply having regard to whether such provision would substantially prejudice the relevant reasonable purpose.

CHAPTER IV
GROUNDS FOR PROCESSING OF SENSITIVE PERSONAL DATA

18. Processing of sensitive personal data based on explicit consent. —

- (1) Sensitive personal data may be processed on the basis of explicit consent.

- (2) For the purposes of sub-section (1), consent shall be considered explicit only if it is valid as per section 12 and is additionally:
- (a) informed, having regard to whether the attention of the data principal has been drawn to purposes or operations in processing that may have significant consequences for the data principal;
 - (b) clear, having regard to whether it is meaningful without recourse to inference from conduct in a context; and
 - (c) specific, having regard to whether the data principal is given the choice of separately consenting to the purposes of, operations in, and the use of different categories of sensitive personal data relevant to processing.

19. Processing of sensitive personal data for certain functions of the State.—

Sensitive personal data may be processed if such processing is strictly necessary for:

- (a) any function of Parliament or any State Legislature.
- (b) the exercise of any function of the State authorised by law for the provision of any service or benefit to the data principal.

20. Processing of sensitive personal data in compliance with law or any order of any court or tribunal.—

Sensitive personal data may be processed if such processing is—

- (a) explicitly mandated under any law made by Parliament or any State Legislature; or
- (b) necessary for compliance with any order or judgment of any Court or Tribunal in India.

21. Processing of certain categories of sensitive personal data for prompt action.—

Passwords, financial data, health data, official identifiers, genetic data, and biometric data may be processed where such processing is strictly necessary—

- (a) to respond to any medical emergency involving a threat to the life or a severe threat to the health of the data principal;
- (b) 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; or
- (c) to undertake any measure to ensure safety of, or provide assistance or services to, any individual during any disaster or any breakdown of public order.

22. Further categories of sensitive personal data.—

- (1) Such further categories of personal data as may be specified by the Authority shall be sensitive personal data and, where such categories of personal data have been specified, the Authority may also specify any further grounds on which such specified categories of personal data may be processed.
- (2) The Authority shall specify categories of personal data under sub-section (1) having regard to—
 - (a) the risk of significant harm that may be caused to the data principal by the processing of such category of personal data;
 - (b) the expectation of confidentiality attached to such category of personal data;
 - (c) whether a significantly discernible class of data principals may suffer significant harm from the processing of such category of personal data; and
 - (d) the adequacy of protection afforded by ordinary provisions applicable to personal data.
- (3) The Authority may also specify categories of personal data, which require additional safeguards or restrictions where repeated, continuous or systematic collection for the purposes of profiling takes place and, where such categories of personal data have been specified, the Authority may also specify such additional safeguards or restrictions applicable to such processing.

CHAPTER V
PERSONAL AND SENSITIVE PERSONAL DATA OF CHILDREN

23. Processing of personal data and sensitive personal data of children. —

- (1) Every data fiduciary shall process personal data of children in a manner that protects and advances the rights and best interests of the child.
- (2) Appropriate mechanisms for age verification and parental consent shall be incorporated by data fiduciaries in order to process personal data of children.
- (3) Appropriateness of an age verification mechanism incorporated by a data fiduciary shall be determined on the basis of—
 - (a) volume of personal data processed;
 - (b) proportion of such personal data likely to be that of children;
 - (c) possibility of harm to children arising out of processing of personal data; and
 - (d) such other factors as may be specified by the Authority.

- (4) The Authority shall notify the following as guardian data fiduciaries—
 - (a) data fiduciaries who operate commercial websites or online services directed at children; or
 - (b) data fiduciaries who process large volumes of personal data of children.
- (5) Guardian data fiduciaries shall be barred from profiling, tracking, or behavioural monitoring of, or targeted advertising directed at, children and undertaking any other processing of personal data that can cause significant harm to the child.
- (6) Sub-section (5) may apply in such modified form, to data fiduciaries offering counseling or child protection services to a child, as the Authority may specify.
- (7) Where a guardian data fiduciary notified under sub-section (4) exclusively provides counseling or child protection services to a child, as under sub-section (6), then such guardian data fiduciary will not be required to obtain parental consent as set out under sub-section (2).

CHAPTER VI DATA PRINCIPAL RIGHTS

24. Right to confirmation and access.—

- (1) The data principal shall have the right to obtain from the data fiduciary—
 - (a) confirmation whether the data fiduciary is processing or has processed personal data of the data principal;
 - (b) a brief summary of the personal data of the data principal being processed or that has been processed by the data fiduciary;
 - (c) a brief summary of processing activities undertaken by the data fiduciary with respect to the personal data of the data principal, including any information provided in the notice under section 8 in relation to such processing activities.
- (2) The data fiduciary shall provide the information as required under this section to the data principal in a clear and concise manner that is easily comprehensible to a reasonable person.

25. Right to correction, etc.—

- (1) Where necessary, having regard to the purposes for which personal data is being processed, the data principal shall have the right to obtain from the data fiduciary processing personal data of the data principal—

- (a) the correction of inaccurate or misleading personal data;
 - (b) the completion of incomplete personal data; and
 - (c) the updating of personal data that is out of date.
- (2) Where the data fiduciary receives a request under sub-section (1), and the data fiduciary does not agree with the need for such correction, completion or updating having regard to the purposes of processing, the data fiduciary shall provide the data principal with adequate justification in writing for rejecting the application.
- (3) Where the data principal is not satisfied with the justification provided by the data fiduciary under sub-section (2), the data principal may require that the data fiduciary take reasonable steps to indicate, alongside the relevant personal data, that the same is disputed by the data principal.
- (4) Where the data fiduciary corrects, completes, or updates personal data in accordance with sub-section (1), the data fiduciary shall also take reasonable steps to notify all relevant entities or individuals to whom such personal data may have been disclosed regarding the relevant correction, completion or updating, particularly where such action would have an impact on the rights and interests of the data principal or on decisions made regarding them.

26. Right to Data Portability.—

- (1) The data principal shall have the right to—
- (a) receive the following personal data related to the data principal in a structured, commonly used and machine-readable format—
 - (i) which such data principal has provided to the data fiduciary;
 - (ii) which has been generated in the course of provision of services or use of goods by the data fiduciary; or
 - (iii) which forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained.
 - (b) have the personal data referred to in clause (a) transferred to any other data fiduciary in the format referred to in that clause.
- (2) Sub-section (1) shall only apply where the processing has been carried out through automated means, and shall not apply where—
- (a) processing is necessary for functions of the State under section 13;
 - (b) processing is in compliance of law as referred to in section 14; or
 - (c) compliance with the request in sub-section (1) would reveal a trade secret of any data fiduciary or would not be technically feasible.

27. Right to Be Forgotten.—

- (1) The data principal shall have the right to restrict or prevent continuing disclosure of personal data by a data fiduciary related to the data principal where such disclosure—
 - (a) has served the purpose for which it was made or is no longer necessary;
 - (b) was made on the basis of consent under section 12 and such consent has since been withdrawn; or
 - (c) was made contrary to the provisions of this Act or any other law made by Parliament or any State Legislature.
- (2) Sub-section (1) shall only apply where the Adjudicating Officer under section 68 determines the applicability of clause (a), (b) or (c) of sub-section (1) and that the rights and interests of the data principal in preventing or restricting the continued disclosure of personal data override the right to freedom of speech and expression and the right to information of any citizen.
- (3) In determining whether the condition in sub-section (2) is satisfied, the Adjudicating Officer shall have regard to—
 - (a) the sensitivity of the personal data;
 - (b) the scale of disclosure and the degree of accessibility sought to be restricted or prevented;
 - (c) the role of the data principal in public life;
 - (d) the relevance of the personal data to the public; and
 - (e) the nature of the disclosure and of the activities of the data fiduciary, particularly whether the data fiduciary systematically facilitates access to personal data and whether the activities would be significantly impeded if disclosures of the relevant nature were to be restricted or prevented.
- (4) The right under sub-section (1) shall be exercised by filing an application in such form and manner as may be prescribed.
- (5) Where any person finds that personal data, the disclosure of which has been restricted or prevented by an order of the Adjudicating Officer under sub-section (2) does not satisfy the conditions referred to in that sub-section any longer, they may apply for the review of that order to the Adjudicating Officer in such manner as may be prescribed, and such Adjudicating Officer shall review her order on the basis of the considerations referred to in sub-section (3).

28. General conditions for the exercise of rights in this Chapter.—

- (1) The exercise of any right under this Chapter, except the right under section 27, shall only be on the basis of a request made in writing to the data fiduciary with reasonable information to satisfy the data fiduciary of the identity of the data principal making the request and the data fiduciary shall acknowledge receipt of such request within such period of time as may be specified.

- (2) The data fiduciary may charge a reasonable fee to be paid for complying with requests made under this Chapter, except for requests made under clauses (a) and (b) of sub-section (1) of section 24 and section 25 which shall be complied with by the data fiduciary without charging any fee.
- (3) The Authority may specify a reasonable time period within which the data fiduciary shall comply with the requests under this Chapter, and such time period shall be communicated to the data principal along with the acknowledgement referred to in sub-section (1).
- (4) Where any request made under this Chapter is refused by the data fiduciary, it shall provide the data principal making such request with adequate reasons for such refusal as per the provisions of this Chapter in writing, and shall inform the data principal regarding the right to file a complaint with the Authority against the refusal within such period and in such manner as may be specified.
- (5) The data fiduciary is not obliged to comply with any request made under this Chapter where such compliance would harm the rights of any other data principal under this Act.
- (6) The manner of exercise of rights under this Chapter shall be in such form as may be provided by law or in the absence of such law, in a reasonable format to be followed by each data fiduciary.

CHAPTER VII

TRANSPARENCY AND ACCOUNTABILITY MEASURES

29. Privacy by Design. —

Every data fiduciary shall implement policies and measures to ensure that—

- (a) managerial, organisational, business practices and technical systems are designed in a manner to anticipate, identify and avoid harm to the data principal;
- (b) the obligations mentioned in Chapter II are embedded in organisational and business practices;
- (c) technology used in the processing of personal data is in accordance with commercially accepted or certified standards;
- (d) legitimate interests of businesses including any innovation is achieved without compromising privacy interests;
- (e) privacy is protected throughout processing from the point of collection to deletion of personal data;
- (f) processing of personal data is carried out in a transparent manner; and
- (g) the interest of the data principal is accounted for at every stage of processing of personal data.

30. Transparency.—

- (1) The data fiduciary shall take reasonable steps to maintain transparency regarding its general practices related to processing personal data and shall make the following information available in an easily accessible form as may be specified—
 - (a) the categories of personal data generally collected and the manner of such collection;
 - (b) the purposes for which personal data is generally processed;
 - (c) any categories of personal data processed in exceptional situations or any exceptional purposes of processing that create a risk of significant harm;
 - (d) the existence of and procedure for the exercise of data principal rights mentioned in Chapter VI, and any related contact details for the same;
 - (e) the existence of a right to file complaints to the Authority;
 - (f) where applicable, any rating in the form of a data trust score that may be accorded to the data fiduciary under section 35;
 - (g) where applicable, information regarding cross-border transfers of personal data that the data fiduciary generally carries out; and
 - (h) any other information as may be specified by the Authority.
- (2) The data fiduciary shall notify the data principal of important operations in the processing of personal data related to the data principal through periodic notifications in such manner as may be specified.

31. Security Safeguards.—

- (1) Having regard to the nature, scope and purpose of processing personal data undertaken, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, the data fiduciary and the data processor shall implement appropriate security safeguards including—
 - (a) use of methods such as de-identification and encryption;
 - (b) steps necessary to protect the integrity of personal data; and
 - (c) steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data.
- (2) Every data fiduciary and data processor shall undertake a review of its security safeguards periodically as may be specified and may take appropriate measures accordingly.

32. Personal Data Breach.—

- (1) The data fiduciary shall notify the Authority of any personal data breach relating to any personal data processed by the data fiduciary where such breach is likely to cause harm to any data principal.

- (2) The notification referred to in sub-section (1) shall include the following particulars—
 - (a) nature of personal data which is the subject matter of the breach;
 - (b) number of data principals affected by the breach;
 - (c) possible consequences of the breach; and
 - (d) measures being taken by the data fiduciary to remedy the breach.
- (3) The notification referred to in sub-section (1) shall be made by the data fiduciary to the Authority as soon as possible and not later than the time period specified by the Authority, following the breach after accounting for any time that may be required to adopt any urgent measures to remedy the breach or mitigate any immediate harm.
- (4) Where it is not possible to provide all the information as set out in sub-section (2) at the same time, the data fiduciary shall provide such information to the Authority in phases without undue delay.
- (5) Upon receipt of notification, the Authority shall determine whether such breach should be reported by the data fiduciary to the data principal, taking into account the severity of the harm that may be caused to such data principal or whether some action is required on the part of the data principal to mitigate such harm.
- (6) The Authority, may in addition to requiring the data fiduciary to report the personal data breach to the data principal under sub-section (5), direct the data fiduciary to take appropriate remedial action as soon as possible and to conspicuously post the details of the personal data breach on its website.
- (7) The Authority may, in addition, also post the details of the personal data breach on its own website.

33. Data Protection Impact Assessment.—

- (1) Where the data fiduciary intends to undertake any processing involving new technologies or large scale profiling or use of sensitive personal data such as genetic data or biometric data, or any other processing which carries a risk of significant harm to data principals, such processing shall not be commenced unless the data fiduciary has undertaken a data protection impact assessment in accordance with the provisions of this section.
- (2) The Authority may, in addition, specify those circumstances, or classes of data fiduciaries, or processing operations where such data protection impact assessment shall be mandatory, and may also specify those instances where a data auditor under this Act shall be engaged by the data fiduciary to undertake a data protection impact assessment.
- (3) A data protection impact assessment shall contain, at a minimum—
 - (a) detailed description of the proposed processing operation, the purpose of processing and the nature of personal data being processed;

- (b) assessment of the potential harm that may be caused to the data principals whose personal data is proposed to be processed; and
 - (c) measures for managing, minimising, mitigating or removing such risk of harm.
- (4) Upon completion of the data protection impact assessment, the data protection officer shall review the assessment prepared and shall submit the same to the Authority in such manner as may be specified.
- (5) On receipt of the assessment, if the Authority has reason to believe that the processing is likely to cause harm to the data principals, the Authority may direct the data fiduciary to cease such processing or direct that such processing shall be subject to such conditions as may be issued by the Authority.

34. Record-Keeping. —

- (1) The data fiduciary shall maintain accurate and up-to-date records of the following—
 - (a) important operations in the data life-cycle including collection, transfers, and erasure of personal data to demonstrate compliance as required under section 11;
 - (b) periodic review of security safeguards under section 31;
 - (c) data protection impact assessments under section 33; and
 - (d) any other aspect of processing as may be specified by the Authority.
- (2) The records in sub-section (1) shall be maintained in such form as specified by the Authority.
- (3) Notwithstanding anything contained in this Act, this section shall apply to the Central or State Government, departments of the Central and State Government, and any agency instrumentality or authority which is “the State” under Article 12 of the Constitution.

35. Data Audits. —

- (1) The data fiduciary shall have its policies and the conduct of its processing of personal data audited annually by an independent data auditor under this Act.
- (2) The data auditor will evaluate the compliance of the data fiduciary with the provisions of this Act, including—
 - (a) clarity and effectiveness of notices under section 8;
 - (b) effectiveness of measures adopted under section 29;
 - (c) transparency in relation to processing activities under section 30;
 - (d) security safeguards adopted pursuant to section 31;
 - (e) instances of personal data breach and response of the data fiduciary, including the promptness of notification to the Authority under section 32; and
 - (f) any other matter as may be specified.

- (3) The Authority shall specify the form, manner and procedure for conducting audits under this section including any civil penalties on data auditors for negligence.
- (4) The Authority shall register persons with expertise in the area of information technology, computer systems, data science, data protection or privacy, with such qualifications, experience and eligibility having regard to factors such as independence, integrity and ability, as it may specify, as data auditors under this Act.
- (5) A data auditor may assign a rating in the form of a data trust score to the data fiduciary pursuant to a data audit conducted under this section.
- (6) The Authority shall specify the criteria for assigning a rating in the form of a data trust score having regard to the factors mentioned in sub-section (2).
- (7) Notwithstanding sub-section (1) where the Authority is of the view that the data fiduciary is processing personal data in a manner that is likely to cause harm to a data principal, the Authority may order the data fiduciary to conduct an audit and shall appoint a data auditor for that purpose.

36. Data Protection Officer.—

- (1) The data fiduciary shall appoint a data protection officer for carrying out the following functions—
 - (a) providing information and advice to the data fiduciary on matters relating to fulfilling its obligations under this Act;
 - (b) monitoring personal data processing activities of the data fiduciary to ensure that such processing does not violate the provisions of this Act;
 - (c) providing advice to the data fiduciary where required on the manner in which data protection impact assessments must be carried out, and carry out the review of such assessment as under sub-section (4) of section 33;
 - (d) providing advice to the data fiduciary, where required on the manner in which internal mechanisms may be developed in order to satisfy the principles set out under section 29;
 - (e) providing assistance to and cooperating with the Authority on matters of compliance of the data fiduciary with provisions under this Act;
 - (f) act as the point of contact for the data principal for the purpose of raising grievances to the data fiduciary pursuant to section 39 of this Act; and
 - (g) maintaining an inventory of all records maintained by the data fiduciary pursuant to section 34.
- (2) Nothing shall prevent the data fiduciary from assigning any other function to the data protection officer, which it may consider necessary, in addition to the functions provided in sub-section (1) above.

- (3) The data protection officer shall meet the eligibility and qualification requirements to carry out its functions under sub-section (1) as may be specified.
- (4) Where any data fiduciary not present within the territory of India carries on processing to which the Act applies under section 2(2), and the data fiduciary is required to appoint a data protection officer under this Act, the data fiduciary shall appoint such officer who shall be based in India and shall represent the data fiduciary in compliance of obligations under this Act.

37. Processing by entities other than data fiduciaries. —

- (1) The data fiduciary shall only engage, appoint, use or involve a data processor to process personal data on its behalf through a valid contract.
- (2) The data processor referred to in sub-section (1) shall not further engage, appoint, use, or involve another data processor in the relevant processing on its behalf except with the authorisation of the data fiduciary, unless permitted through the contract referred to in sub-section (1).
- (3) The data processor, and any employee of the data fiduciary or the data processor, shall only process personal data in accordance with the instructions of the data fiduciary unless they are required to do otherwise under law and shall treat any personal data that comes within their knowledge as confidential.

38. Classification of data fiduciaries as significant data fiduciaries. —

- (1) The Authority shall, having regard to the following factors, notify certain data fiduciaries or classes of data fiduciaries as significant data fiduciaries—
 - (a) volume of personal data processed;
 - (b) sensitivity of personal data processed;
 - (c) turnover of the data fiduciary;
 - (d) risk of harm resulting from any processing or any kind of processing undertaken by the fiduciary;
 - (e) use of new technologies for processing; and
 - (f) any other factor relevant in causing harm to any data principal as a consequence of such processing.
- (2) The notification of a data fiduciary or classes of data fiduciaries as significant data fiduciaries by the Authority under sub-section (1) shall require such data fiduciary or class of data fiduciaries to register with the Authority in such manner as may be specified.
- (3) All or any of the following obligations in this Chapter, as determined by the Authority, shall apply only to significant data fiduciaries—

- (a) data protection impact assessments under section 33;
 - (b) record-keeping under section 34;
 - (c) data audits under section 35; and
 - (d) data protection officer under section 36.
- (4) Notwithstanding sub-section (3), the Authority may notify the application of all or any of the obligations in sub-section (3) to such data fiduciary or class of data fiduciaries, not being a significant data fiduciary, if it is of the view that any processing activity undertaken by such data fiduciary or class of data fiduciaries carries a risk of significant harm to data principals.

39. Grievance Redressal. —

- (1) Every data fiduciary shall have in place proper procedures and effective mechanisms to address grievances of data principals efficiently and in a speedy manner.
- (2) A data principal may raise a grievance in case of a violation of any of the provisions of this Act, or rules prescribed, or regulations specified thereunder, which has caused or is likely to cause harm to such data principal, 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.
- (3) A grievance raised under sub-section (2) shall be resolved by the data fiduciary in an expeditious manner and no later than thirty days from the date of receipt of grievance by such data fiduciary.
- (4) Where, a grievance under sub-section (2) is not resolved within the time period mentioned under sub-section (3), or where the data principal is not satisfied with the manner in which the grievance is resolved, or the data fiduciary has rejected the grievance raised, the data principal shall have the right to file a complaint with the adjudication wing under section 68 of the Act in the manner prescribed.
- (5) Any person aggrieved by an order made under this section by an Adjudicating Officer in accordance with the procedure prescribed in this regard, may prefer an appeal to the Appellate Tribunal.

CHAPTER VIII
TRANSFER OF PERSONAL DATA OUTSIDE INDIA

40. Restrictions on Cross-Border Transfer of Personal Data. —

- (1) Every data fiduciary shall ensure the storage, on a server or data centre located in India, of at least one serving copy of personal data to which this Act applies.

- (2) The Central Government shall notify categories of personal data as critical personal data that shall only be processed in a server or data centre located in India.
- (3) Notwithstanding anything contained in sub-section (1), the Central Government may notify certain categories of personal data as exempt from the requirement under sub-section (1) on the grounds of necessity or strategic interests of the State.
- (4) Nothing contained in sub-section (3) shall apply to sensitive personal data.

41. Conditions for Cross-Border Transfer of Personal Data. —

- (1) Personal data other than those categories of sensitive personal data notified under sub-section (2) of section 40 may be transferred outside the territory of India where—
 - (a) the transfer is made subject to standard contractual clauses or intra-group schemes that have been approved by the Authority; or
 - (b) the Central Government, after consultation with the Authority, has prescribed that transfers to a particular country, or to a sector within a country or to a particular international organisation is permissible; or
 - (c) the Authority approves a particular transfer or set of transfers as permissible due to a situation of necessity; or
 - (d) in addition to clause (a) or (b) being satisfied, the data principal has consented to such transfer of personal data; or
 - (e) in addition to clause (a) or (b) being satisfied, the data principal has explicitly consented to such transfer of sensitive personal data, which does not include the categories of sensitive personal data notified under sub-section (2) of section 40.
- (2) The Central Government may only prescribe the permissibility of transfers under clause (b) of sub-section (1) where it finds that the relevant personal data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements, and the effectiveness of the enforcement by authorities with appropriate jurisdiction, and shall monitor the circumstances applicable to such data in order to review decisions made under this sub-section.
- (3) Notwithstanding sub-section (2) of Section 40, sensitive personal data notified by the Central Government may be transferred outside the territory of India—
 - (a) to a particular person or entity engaged in the provision of health services or emergency services where such transfer is strictly necessary for prompt action under section 16; and
 - (b) to a particular country, a prescribed sector within a country or to a particular international organisation that has been prescribed under clause (b) of sub-section (1), where the Central Government is satisfied that such transfer or class of

transfersis necessary for any class of data fiduciaries or data principals anddoes not hamper the effective enforcement of this Act.

- (4) Any transfer under clause (a) ofsub-section (3) shall be notified to the Authority within such time period as may be prescribed.
- (5) The Authority may only approve standard contractual clauses or intra-group schemes under clause (a) of sub-section (1) where such clauses or schemes effectively protect the rights of data principals under this Act, including in relation with further transfers from the transferees of personal data under this sub-section to any other person or entity.
- (6) Where a data fiduciary seeks to transfer personal data subject to standard contractual clauses or intra-group schemes under clause (a) of sub-section (1), it shall certify and periodically report to the Authority as may be specified, that the transfer is made under a contract that adheres to such standard contractual clauses or intra-group schemes and that it shall bear any liability for the harm caused due to any non-compliance with the standard contractual clauses or intra-group schemes by the transferee.

CHAPTER IX **EXEMPTIONS**

42. Security of the State.—

- (1) Processing of personal data in the interests of the security of the State shall not be permitted unless it is authorised pursuant to a law, andis in accordance with the procedure established by such law, made by Parliament and is necessary for, and proportionate to, such interests being achieved.
- (2) Any processing authorised by a lawreferred 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.

43. Prevention, detection, investigation and prosecution of contraventions of law.—

- (1) Processing of personal data in the interests of prevention, detection,investigation and prosecution of any offence or any other contravention of law shall not be permitted unless

it is authorised by a law made by Parliament and State Legislature and is necessary for, and proportionate to, such interests being achieved.

- (2) Any processing authorised by 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.
- (3) Sub-section (1) shall apply in relation to processing of personal data of a data principal who is a victim, witness, or any person with information about the relevant offence or contravention only if processing in compliance with the provisions of this law would be prejudicial to the prevention, detection, investigation or prosecution of any offence or other contravention of law.
- (4) Personal data processed under sub-section (1) shall not be retained once the purpose of prevention, detection, investigation or prosecution of any offence or other contravention of law is complete except where such personal data is necessary for the maintenance of any record or database which constitutes a proportionate measure to prevent, detect or investigate or prosecute any offence or class of offences in future.

44. Processing for the purpose of legal proceedings.—

- (1) Where disclosure of personal data is necessary for enforcing any legal right or claim, seeking any relief, defending any charge, opposing any claim, or obtaining any legal advice from an advocate in any impending legal proceeding such processing shall be exempted from the following provisions of this Act—
 - (a) Chapter II, except section 4;
 - (b) Chapter III;
 - (c) Chapter IV;
 - (d) Chapter V;
 - (e) Chapter VI; and
 - (f) Chapter VII, except section 31.
- (2) Where processing of personal data by any Court or Tribunal in India is necessary for the exercise of any judicial function, such processing shall be exempted from the following provisions of this Act—

- (a) Chapter II, except section 4;
- (b) Chapter III;
- (c) Chapter IV;
- (d) Chapter V;
- (e) Chapter VI; and
- (f) Chapter VII, except section 31.

45. Research, archiving or statistical purposes. —

- (1) Where processing of personal data is necessary for research, archiving, or statistical purposes, such processing may be exempted from such provisions of this Act as the Authority may specify except section 4, section 31 and section 33.
- (2) For the purpose of sub-section (1), the Authority may exempt different categories of research, archiving, or statistical purposes from different provisions of the Act.
- (3) Sub-section (1) shall apply only where—
 - (a) compliance with the provisions of this Act will disproportionately divert resources from the purpose referred to in sub-section (1);
 - (b) the purposes of processing cannot be achieved if the personal data is anonymised;
 - (c) the data fiduciary has carried out de-identification meeting the standard contained in any code of practice under section 61, where the purpose of processing can be achieved if the personal data is in a de-identified form;
 - (d) personal data will not be used to take any decision specific to or action directed specifically towards the data principal; and
 - (e) personal data will not be processed in a manner that gives rise to a risk of significant harm to the data principal.

46. Personal or domestic purposes. —

- (1) Personal data processed by a natural person in the course of a purely personal or domestic purpose, shall be exempted from the following provisions of this Act—
 - (a) Chapter II, except section 4;
 - (b) Chapter III;
 - (c) Chapter IV;
 - (d) Chapter V;
 - (e) Chapter VI;
 - (f) Chapter VII; and
 - (g) Chapter VIII.

- (2) Sub-section (1) shall not apply where the relevant processing—
- (a) involves disclosure to the public; or
 - (b) is undertaken in connection with any professional or commercial activity.

47. Journalistic purposes.—

- (1) Where the processing of personal data is necessary for or relevant to a journalistic purpose, the following provisions of the Act shall not apply—
- (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.
- (2) Sub-section (1) shall apply only where it can be demonstrated that the processing is in compliance with any code of ethics issued by—
- (a) the Press Council of India, or
 - (b) any media self-regulatory organisation

48. Manual processing by small entities.—

- (1) Subject to any law for the time being in force, where personal data is processed through means other than automated means by a small entity, the following provisions of the Act shall not apply—
- (a) Sections 8, 9 and 10 in Chapter II;
 - (b) Clause (c) of sub-section (1) of section 24, and sections 26 and 27 in Chapter VI; and
 - (c) Section 29 to section 36, and sections 38 and 39 in Chapter VII.
- (2) For the purposes of sub-section (1), a small entity shall be any data fiduciary which—
- (a) did not have a turnover of more than twenty lakh rupees or such other lower amount as may be prescribed by the Central Government in the preceding financial year;
 - (b) does not collect personal data for the purpose of disclosure to any other individuals or entities, including other data fiduciaries or processors; and
 - (c) did not process personal data of more than one hundred data principals in any one day in the preceding twelve calendar months.

Explanation: For the purpose of sub-section (2), “turnover” means the gross amount of revenue recognised in the profit and loss account or any other equivalent statement, as applicable, from the sale, supply or distribution of goods or services or on account of services rendered, or both, by the data fiduciary in the preceding financial year.

CHAPTER X

DATA PROTECTION AUTHORITY OF INDIA

49. Establishment and incorporation of Authority.—

- (1) The Central Government shall, by notification, establish for the purposes of this Act, an Authority to be called the Data Protection Authority of India.
- (2) The Authority shall be a body corporate by the name aforesaid, having perpetual succession and a common seal, with power, subject to the provisions of this Act, to acquire, hold and dispose of property, both movable and immovable, and to contract and shall, by the said name, sue or be sued.
- (3) The head office of the Authority shall be at such place as may be prescribed.
- (4) The Authority may, with the prior approval of the Central Government, establish its offices at other places in India.

50. Composition and qualifications for appointment of members.—

- (1) The Authority shall consist of a chairperson and six whole-time members.
- (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—
 - (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; and
 - (c) one expert of repute as mentioned in sub-section (6), to be nominated by the Chief Justice of India or a judge of the Supreme Court of India nominated by the Chief Justice of India, in consultation with the Cabinet Secretary.
- (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.
- (4) The chairperson and the members of the Authority shall be persons of ability, integrity and standing, and must have specialised knowledge of, and not less than ten years professional experience in the field of data protection, information technology, data management, data science, data security, cyber and internet laws, and related subjects.

- (5) A vacancy caused to the office of the chairperson or any other member shall be filled up within a period of three months from the date on which such vacancy occurs.
- (6) The Central Government shall maintain a list of at least five experts who have 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.

51. Terms and conditions of appointment.—

- (1) The chairperson and the members shall be appointed for a term of five years or till they attain the age of sixty-five years, whichever is earlier, and they shall not be eligible for re-appointment.
- (2) The salaries and allowances payable to, and other terms and conditions of service of the chairperson and the members shall be such as may be prescribed and shall not be varied to their disadvantage during their term.
- (3) The chairperson and the members shall not, during their term and for a period of two years from the date on which they cease to hold office, accept—
 - (a) any employment either under the Central Government or under any State Government; or
 - (b) any appointment, in any capacity whatsoever, with a significant data fiduciary.
- (4) Notwithstanding anything contained in sub-section (1), the chairperson or a member may—
 - (a) relinquish his office by giving in writing to the Central Government a notice of not less than three months; or
 - (b) be removed from his office in accordance with the provisions of this Act.

52. Removal of members.—

- (1) The Central Government may remove from office, the chairperson or any member who—
 - (a) has been adjudged an insolvent;
 - (b) has become physically or mentally incapable of acting as a chairperson or member;
 - (c) has been convicted of an offence, which in the opinion of the Central Government, involves moral turpitude;
 - (d) has so abused her position as to render her continuation in office detrimental to the public interest; or
 - (e) has acquired such financial or other interest as is likely to affect prejudicially her functions as a chairperson or a member.
- (2) No chairperson or any member shall be removed under clause (d) or (e) of sub-section (1) unless she has been given a reasonable opportunity of being heard.

53. Powers of the chairperson.—

The chairperson shall have powers of general superintendence and direction of the affairs of the Authority and shall also exercise all powers and do all such acts and things which may be exercised or done by the Authority under the Act.

54. Meetings of the Authority.—

- (1) The chairperson and members of the Authority shall meet at such times and places and shall observe such rules and procedures in regard to transaction of business at its meetings including quorum at such meetings, as may be prescribed.
- (2) If, for any reason, the chairperson is unable to attend any meeting of the Authority, any other member chosen by the members present at the meeting, shall preside at the meeting.
- (3) All questions which come up before any meeting of the Authority shall be decided by a majority of votes of the members present and voting, and in the event of an equality of votes, the chairperson or in her absence, the member presiding, shall have a casting or a second vote.
- (4) Any member who has any direct or indirect pecuniary interest in any matter coming up for consideration at a meeting of the Authority shall disclose the nature of her interest at such meeting, which shall be recorded in the proceedings of the Authority and such member shall not take part in any deliberation or decision of the Authority with respect to that matter.

55. Vacancies, etc. not to invalidate proceedings of the Authority.—

No act or proceeding of the Authority shall be invalid merely by reason of—

- (a) any vacancy or defect in the constitution of the Authority;
- (b) any defect in the appointment of a person as a chairperson or member; or,
- (c) any irregularity in the procedure of the Authority not affecting the merits of the case.

56. Officers and Employees of the Authority.—

- (1) The Authority may appoint such officers, employees, consultants and experts as it may consider necessary for effectively discharging its functions under this Act.
- (2) Any remuneration, salary or allowances, and other terms and conditions of service of such officers, employees, consultants and experts shall be such as may be specified.

57. Grants by Central Government.—

The Central Government may, after due appropriation made by Parliament by law in this behalf, make to the Authority grants of such sums of money as it may think fit for the purposes of this Act.

58. Accounts and Audit —

- (1) The Authority shall maintain proper accounts and other relevant records and prepare an annual statement of accounts in such form as may be prescribed by the Central Government in consultation with the Comptroller and Auditor-General of India.
- (2) The accounts of the Authority shall be audited by the Comptroller and Auditor-General of India at such intervals as may be prescribed and any expenditure incurred by her in connection with such audit shall be reimbursed to her by the Authority.
- (3) The Comptroller and Auditor-General of India and any other person appointed by her in connection with the audit of the accounts of the Authority shall have the same rights and privileges and authority in connection with such audit as the Comptroller and Auditor-General of India generally has in connection with the audit of the Government accounts and, in particular, shall have the right to demand the production of books, accounts, connected vouchers and other documents and papers, and to inspect any of the offices of the Authority.
- (4) The accounts of the Authority as certified by the Comptroller and Auditor-General of India or any other person appointed by the Comptroller and Auditor-General of India in this behalf together with the audit report thereon shall be forwarded annually to the Central Government and the Central Government shall cause the same to be laid before each House of the Parliament.

59. Furnishing of returns, etc. to Central Government.—

- (1) The Authority shall furnish to the Central Government at such time and in such form and manner as may be prescribed or as the Central Government may direct, such returns and statements and such particulars in regard to any proposed or existing programme for the promotion and development of protection of personal data, as the Central Government from time to time, require.
- (2) The Authority shall prepare once every year in such form and at such time as may be prescribed, an annual report giving a summary of its activities during the previous year and copies of the report shall be forwarded to the Central Government.

- (3) A copy of the report received under sub-section (2) shall be laid, as soon as may be after it is received, before each House of the Parliament.

60. Powers and Functions of the Authority.—

- (1) It shall be the duty of the Authority to protect the interests of data principals, prevent any misuse of personal data, ensure compliance with the provisions of this Act, and promote awareness of data protection.
- (2) Without prejudice to the generality of the foregoing and other functions set out under this Act, the functions of the Authority shall include—
- (a) monitoring and enforcing application of the provisions of this Act;
 - (b) specifying reasonable purposes for which personal data may be processed under section 17 of this Act;
 - (c) specifying residuary categories of sensitive personal data under section 22 of this Act;
 - (d) taking prompt and appropriate action in response to a data security breach in accordance with the provisions of this Act;
 - (e) specifying the circumstances where a data protection impact assessment may be required to be undertaken in accordance with section 33 of this Act;
 - (f) maintaining a database on its website containing names of significant data fiduciaries along with a rating in the form of a data trust score indicating compliance with the obligations of this Act by such fiduciaries;
 - (g) specifying the criteria for assigning a rating in the form of a data trust score by a data auditor having regard to the factors mentioned in sub-section (2) of section 35;
 - (h) examination of any data audit reports submitted under section 35 of this Act and taking any action pursuant thereto in accordance with the provisions of this Act;
 - (i) issuance of a certificate of registration to data auditors and renewal, modification, withdrawal, suspension or cancellation thereof and maintaining a database on its website of such registered data auditors and specifying the requisite qualifications, code of conduct, practical training and functions to be performed by such data auditors;
 - (j) categorisation and issuance of certificate of registration to significant data fiduciaries and renewal, modification, withdrawal, suspension or cancellation thereof under section 38;
 - (k) monitoring cross-border transfer of personal data under section 41 of this Act;
 - (l) issuing codes of practice in accordance with section 61 of this Act and publishing such codes on its website;
 - (m) promoting public awareness and understanding of the risks, rules, safeguards and rights in respect of protection of personal data, including issuance of any public statement setting out trends in, or specific instances of, contravention of the

- provisions of this Act by a data fiduciary or a class of data fiduciaries, as the case may be;
- (n) promoting awareness among data fiduciaries of their obligations and duties under this Act;
 - (o) monitoring technological developments and commercial practices that may affect protection of personal data;
 - (p) promoting measures and undertaking research for innovation in the field of protection of personal data;
 - (q) advising Parliament, Central Government, State Government and any regulatory or statutory authority on measures that must be undertaken to promote protection of personal data and ensuring consistency of application and enforcement of this Act;
 - (r) issuing guidance on any provision under this Act either on its own or in response to any query received from a data fiduciary where the Authority considers it necessary, subject always to the provisions of this Act;
 - (s) advising the Central Government on the acceptance of any relevant international instrument relating to protection of personal data;
 - (t) specifying fees and other charges for carrying out the purposes of this Act;
 - (u) receiving and handling complaints under the provisions of this Act;
 - (v) calling for information from, conducting inspections and inquiries into the affairs of data fiduciaries in accordance with the provisions of this Act;
 - (w) preparation and publication of reports setting out the result of any inspection or inquiry and any other comments that the Authority deems to be in public interest; and
 - (x) performing such other functions, including maintaining, updating and submitting any records, documents, books, registers or any other data, as may be prescribed.
- (3) Notwithstanding anything contained in any other law for the time being in force, while exercising the powers under clause (v) of sub-section (2), the Authority shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908) while trying a suit, in respect of the following matters, namely—
- (a) the discovery and production of books of account and other documents, at such place and at such time as may be specified;
 - (b) summoning and enforcing the attendance of persons and examining them on oath;
 - (c) inspection of any book, document, register or record of any data fiduciary;
 - (d) issuing commissions for the examination of witnesses or documents;
 - (e) any other matter which may be prescribed.
- (4) Where, pursuant to the provisions of this Act, the Authority processes personal data, it shall be construed as the data fiduciary or the data processor in relation to such personal data as applicable, and where the Authority comes into possession of any information that

is treated as confidential by the data fiduciary or data processor, it shall not disclose such information unless required as per law, or where it is required to carry out its function under clause (w) of sub-section (2).

61. Codes of Practice.—

- (1) The Authority shall issue codes of practice in accordance with this section to promote good practices of data protection and facilitate compliance with the obligations under this Act.
- (2) Notwithstanding sub-section (1), the Authority may also approve, and issue codes of practice submitted by an industry or trade association, an association representing the interest of data principals, any sectoral regulator or statutory authority, or any departments or ministries of the Central or State Government.
- (3) The Authority shall ensure transparency while approving or issuing any code of practice under this section in accordance with sub-section (4).
- (4) A code of practice, whether under sub-section (1) or sub-section (2), shall not be issued unless the Authority has undertaken a requisite consultation process with relevant sectoral regulators and stakeholders including the public and has followed the procedure for issuance of such code of practice, as may be prescribed.
- (5) A code of practice issued under this section shall not derogate from the provisions of this Act or any applicable law.
- (6) Without prejudice to sub-sections (1) or (2), or any other provision of this Act, the Authority may issue codes of practice in respect of the following matters—
 - (a) requirements for notice under section 8 of this Act including any model forms or guidance relating to notice;
 - (b) measures for ensuring quality of personal data processed under section 9 of this Act;
 - (c) measures pertaining to the retention of personal data under section 10 of this Act;
 - (d) conditions for valid consent under section 12 of this Act;
 - (e) processing of personal data under section 15 of this Act;
 - (f) activities where processing of personal data may be undertaken under section 17;
 - (g) processing of sensitive personal data under Chapter IV of this Act;
 - (h) processing of personal data under any other ground for processing, including processing of personal data of children and development of appropriate age-verification mechanisms under section 23 and mechanisms for processing personal data on the basis of consent of users incapable of providing valid consent under this Act;
 - (i) exercise of any right by data principals under Chapter VI of this Act;
 - (j) the standards and means by which a data principal may avail the right to data portability under section 26 of this Act;

- (k) transparency and accountability measures including the standards thereof to be maintained by data fiduciaries and data processors under Chapter VII of this Act;
 - (l) standards for security safeguards to be maintained by data fiduciaries and data processors under section 31 of this Act;
 - (m) methods of de-identification and anonymisation;
 - (n) methods of destruction, deletion, or erasure of personal data where required under this Act;
 - (o) appropriate action to be taken by the data fiduciary or data processor in response to a personal data breach under section 32 of this Act;
 - (p) manner in which data protection impact assessments may be carried out by the data fiduciary or a class thereof under section 33 of this Act;
 - (q) cross-border transfer of personal data pursuant to section 41 of this Act;
 - (r) processing of any personal data or sensitive personal data to carry out any activity necessary for research, archiving or statistical purposes under section 45 of this Act; and
 - (s) any other matter which, in the view of the Authority, may require issuance of a code of practice.
- (7) Non-compliance by the data fiduciary or data processor with any code of practice issued under this section and applicable to it may be considered by the Authority, or any court, tribunal or statutory body, while determining whether such data fiduciary or data processor has violated the provisions of this Act.
- (8) Nothing contained in sub-section (7) shall prevent a data fiduciary or data processor from demonstrating before the Authority, or any court, tribunal or statutory body, that it has adopted an equivalent or a higher standard than that stipulated under the relevant code of practice.
- (9) The Authority may review, modify or revoke a code of practice issued under this section in the manner prescribed.
- (10) The Authority shall maintain a register in the manner prescribed containing details of the codes of practice, which are currently in force and shall make such codes of practice publicly available on its website.

62. Power of Authority to issue directions.—

- (1) The Authority may, for the discharge of its functions under this Act, issue such directions from time to time as it may consider necessary to data fiduciaries or data processors generally, or to any data fiduciary or data processor in particular, and such data fiduciaries or data processors, as the case may be, shall be bound to comply with such directions.
- (2) No such direction shall be issued under sub-section (1) unless the Authority has given a reasonable opportunity of being heard to the data fiduciaries or data processors concerned.

- (3) The Authority may, on a representation made to it or on its own motion, modify, suspend, withdraw or cancel any direction issued under sub-section (1) and in doing so, may impose such conditions as it thinks fit, subject to which the modification, suspension, withdrawal or cancellation shall have effect.

63. Power of Authority to call for information.—

- (1) Without prejudice to the other provisions of this Act, the Authority may require a data fiduciary or data processor to provide such information as may be reasonably required by it for discharging its functions under this Act.
- (2) If the Authority requires a data fiduciary or a data processor to provide information as per sub-section (1), it must provide a written notice to the data fiduciary or the data processor stating the reasons for such requisition.
- (3) The Authority shall specify the manner in which the data fiduciary or data processor shall provide the information sought in sub-section (1), including the designation of the officer or employee of the Authority who may seek such information, time frame within which such information is required to be furnished and the form in which such information may be provided.

64. Power of Authority to conduct inquiry. —

- (1) The Authority may conduct an inquiry where it has reasonable grounds to believe that—
 - (a) the activities of the data fiduciary or data processor being conducted in a manner which is detrimental to the interest of data principals; or
 - (b) any data fiduciary or data processor has violated any of the provisions of this Act or the rules prescribed, or the regulations specified, or directions issued by the Authority thereunder.
- (2) For the purpose of sub-section (1), the Authority shall, by an order in writing, appoint one of its officers as an Inquiry Officer to inquire into the affairs of such data fiduciary or data processor and to report to the Authority on any inquiry made.
- (3) An Inquiry Officer, may wherever necessary, appoint any other person for the purpose of assisting in any inquiry under this section.
- (4) The order referred to in sub-section (2) shall also set out the reasons for commencing the inquiry and the scope of the inquiry and may be modified from time to time.
- (5) Every officer, employee or other person acting under the direct authority of the data fiduciary or the data processor, or a service provider, or a contractor, where services are being obtained by or provided to the data fiduciary or data processor, as the case may be,

shall be bound to produce before the Inquiry Officer directed to make the inquiry, all such books, registers, documents, records and any data in their custody or power and to furnish to the Inquiry Officer any statement and information relating to the affairs of the data fiduciary or data processor as the Inquiry Officer may require within such time as the said Inquiry Officer may specify.

- (6) The Inquiry Officer shall undertake the inquiry only after providing a written notice to the persons referred to in sub-section (5) stating the reasons for the inquiry and the relationship between the data fiduciary and the scope of the inquiry.
- (7) The Inquiry Officer may keep in its custody any books, registers, documents, records and other data produced under sub-section (5) for six months and thereafter shall return the same to the person by whom or on whose behalf such books, registers, documents, record and data are produced, unless an approval to retain such books, registers, documents, record and data for an additional period not exceeding three months has been obtained from the Authority.
- (8) Without prejudice to any other power set out in this Act or under any other law, any Inquiry Officer directed to make an inquiry may examine on oath, any officer, employee or other person acting under the direct authority of the data fiduciary or the data processor, or a service provider, or a contractor where services are being obtained by or provided to the data fiduciary or data processor, as the case may be, in relation to the business or activity of the data fiduciary or data processor.

65. Action to be taken by Authority pursuant to an inquiry.—

- (1) On receipt of a report under sub-section (2) of section 64, the Authority may, after giving such opportunity to the data fiduciary or data processor to make a representation in connection with the report as the Authority deems reasonable, by an order in writing—
 - (a) issue a warning to the data fiduciary or data processor where the business or activity is likely to violate the provisions of this Act;
 - (b) issue a reprimand to the data fiduciary or data processor where the business or activity has violated the provisions of this Act;
 - (c) require the data fiduciary or data processor to cease and desist from committing or causing any violation of the provisions of this Act;
 - (d) require the data fiduciary or data processor to modify its business or activity to bring it in compliance with the provisions of this Act;
 - (e) temporarily suspend or discontinue business or activity of the data fiduciary or data processor which is in contravention of the provisions of this Act;
 - (f) vary, suspend or cancel any registration granted by the Authority in case of a significant data fiduciary;
 - (g) suspend or discontinue any cross-border flow of personal data; or
 - (h) require the data fiduciary or data processor to take any such action in respect of any matter arising out of the report as the Authority may think fit.

- (2) A data fiduciary or data processor aggrieved by an order made under this section by the Authority may prefer an appeal to the Appellate Tribunal.

66. Search and Seizure.—

- (1) Where the Authority has reasonable grounds to believe that—
- (a) any person who has been required under sub-section (5) of section 64 to produce, or cause to be produced, any books, registers, documents, records or data in her custody or power is likely to omit or fail, or has omitted or failed, to do so; or
 - (b) any books, registers, documents, records or data belonging to any person as mentioned in clause(a) of sub-section (1) are likely to be tampered with, altered, mutilated, manufactured, falsified or destroyed; or
 - (c) a contravention of any provision of this Act has been committed or is likely to be committed by a data fiduciary,

it may authorise any officer of the Authority not below the rank equivalent to that of a Gazetted Officer of the Central Government (hereinafter referred to as “Authorised Officer”) to—

- (i) enter and search any building or place where she has reason to suspect that such books, registers, documents, records or data are kept;
 - (ii) break open the lock of any box, locker, safe, almirah or other receptacle for exercising the powers conferred by clause (i) where the keys thereof are not available;
 - (iii) access any computer, computer resource, or any other device containing or suspected to be containing data;
 - (iv) seize all or any such books, registers, documents, records or data found as a result of such search;
 - (v) place marks of identification on such books, registers, documents, records or databases or make extracts or copies of the same.
- (2) The Authorised Officer may requisition the services of any police officer or of any officer of the Central Government, or of both, as the case may be, for assistance related to any of the purposes specified in sub-section (1) and it shall be the duty of every such police officer or officer to comply with such requisition.
- (3) The Authorised Officer may, where it is not practicable to seize any such book, register, document, record or data specified in sub-section (1), serve an order on the person who is in immediate possession or control thereof that such person shall not remove, part with or otherwise deal with it except with the previous permission of such officer and such officer may take such steps as may be necessary for ensuring compliance with this sub-section.
- (4) The Authorised Officer may, during the course of the search or seizure, examine on oath any person who is found to be in possession or control of any books, registers,

documents, records or data, and any statement made by such person during such examination may thereafter be used in evidence in any proceeding under this Act.

- (5) The books, registers, documents, records or data seized under sub-section (1) shall not be retained by the Authorised Officer for a period exceeding six months from the date of the seizure unless the reasons for retaining the same are recorded by her in writing and the approval of the Authority for such retention is obtained.
- (6) The Authority shall not authorise the retention of the books, registers, documents, records or data for a period exceeding thirty days after all the proceedings under this Act, for which the said books, registers, documents, records or data are relevant, are completed.
- (7) The person from whose custody the books, registers, documents, records or data are seized under sub-section (1) may make copies thereof, or take extracts therefrom, in the presence of the Authorised Officer or any other person appointed by her in this behalf at such place and time as the Authorised Officer may designate in this behalf.
- (8) If a person legally entitled to the books, registers, documents, records or data seized under sub-section (1) objects for any reason to the approval given by the Authority under sub-section (5), such person may make an application to the Appellate Tribunal stating therein the reason for such objection and requesting for the return of the books, registers, documents, records or data.
- (9) On receipt of the application under sub-section (8), the Appellate Tribunal may, after giving the parties an opportunity of being heard, pass such order as it thinks fit including any order prohibiting the destruction or alteration of such books, registers, documents, records or data.
- (10) The provisions of the Code of Criminal Procedure, 1973 (2 of 1974) relating to searches and seizures shall apply, so far as may be, to every search and seizure made under sub-section (1).
- (11) Without prejudice to the generality of the foregoing, rules may be prescribed in relation to the process for search and seizure under this section and in particular may provide for—
 - (a) obtaining ingress into such building or place to be searched where free ingress thereto is not available;
 - (b) obtaining access to a computer, computer resource, or any other device containing or suspected to be containing data, where such access is not available;
 - (c) ensuring safe custody of any books, registers, documents, records or data seized under this section.

67. Coordination between the Authority and other regulators or authorities.—

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.

68. Appointment of Adjudicating Officer.—

- (1) Without prejudice to any other provision of this Act and for the purpose of imposing of penalties under section 69 to section 73 or awarding compensation under section 75, the Authority shall have a separate adjudication wing.
- (2) The Central Government shall, having regard to the need to ensure the operational segregation, independence, and neutrality of the adjudication wing, prescribe—
 - (a) number of Adjudicating Officers;
 - (b) qualification of Adjudicating Officers;
 - (c) manner and terms of appointment of Adjudicating Officers ensuring independence of such officers;
 - (d) jurisdiction of Adjudicating Officers;
 - (e) procedure for carrying out an adjudication under this Act; and
 - (f) other such requirements as the Central Government may deem fit.
- (3) The Adjudicating Officers shall be persons of ability, integrity and standing, and must have specialised knowledge of, and not less than seven years professional experience in the fields of constitutional law, cyber and internet laws, information technology law and policy, data protection and related subjects.

CHAPTER XI
PENALTIES AND REMEDIES

69. Penalties.—

- (1) Where the data fiduciary contravenes any of the following provisions, it shall be liable to a penalty which may extend up to five crore rupees or two per cent of its total worldwide turnover of the preceding financial year, whichever is higher, as applicable—
 - (a) obligation to take prompt and appropriate action in response to a data security breach under section 32 of this Act;
 - (b) obligation to undertake a data protection impact assessment by a significant data fiduciary under section 33 of this Act;
 - (c) obligation to conduct a data audit by a significant data fiduciary under section 35 of this Act;
 - (d) appointment of a data protection officer by a significant data fiduciary under section 36 of this Act;
 - (e) failure to register with the Authority under sub-section (2) of section 38.

- (2) Where a data fiduciary contravenes any of the following provisions, it shall be liable to a penalty which may extend up to fifteen crore rupees or four per cent of its total worldwide turnover of the preceding financial year, whichever is higher, as applicable—
- (a) processing of personal data in violation of the provisions of Chapter II;
 - (b) processing of personal data in violation of the provisions of Chapter III;
 - (c) processing of sensitive personal data in violation of the provisions of Chapter IV of this Act;
 - (d) processing of personal data of children in violation of the provisions of Chapter V;
 - (e) failure to adhere to security safeguards as per section 31 of this Act;
 - (f) transfer of personal data outside India in violation of section 41 of this Act.

Explanation I. For the purposes of this section, “total worldwide turnover” means the gross amount of revenue recognised in the profit and loss account or any other equivalent statement, as applicable, from the sale, supply or distribution of goods or services or on account of services rendered, or both, and where such revenue is generated within India and outside India.

Explanation II. For the purposes of this section, it is hereby clarified that total worldwide turnover in relation to a data fiduciary is the total worldwide turnover of the data fiduciary and the total worldwide turnover of any group entity of the data fiduciary where such turnover of a group entity arises as a result of the processing activities of the data fiduciary, having regard to factors, including—

- (i) the alignment of the overall economic interests of the data fiduciary and the group entity;
- (ii) the relationship between the data fiduciary and the group entity specifically in relation to the processing activity undertaken by the data fiduciary; and
- (iii) the degree of control exercised by the group entity over the data fiduciary or vice versa, as the case may be.

70. Penalty for failure to comply with data principal requests under Chapter VI.—

Where, any data fiduciary, without any reasonable explanation, fails to comply with any request made by a data principal under Chapter VI of this Act, such data fiduciary shall be liable to a penalty of five thousand rupees for each day during which such default continues, subject to a maximum of ten lakh rupees in case of significant data fiduciaries and five lakh rupees in other cases.

71. Penalty for failure to furnish report, returns, information, etc.—

If any data fiduciary, who is required under this Act, or rules prescribed or regulations specified thereunder, to furnish any report, return or information to the Authority, fails to furnish the same, then such data fiduciary shall be liable to penalty which shall be ten thousand rupees for each day during which such default continues, subject to a maximum of twenty lakh rupees in case of significant data fiduciaries and five lakh rupees in other cases.

72. Penalty for failure to comply with direction or order issued by the Authority.—

If any data fiduciary or data processor fails to comply with any direction issued by the Authority under section 62 or order issued by the Authority under section 65, as applicable, such data fiduciary or data processor shall be liable to a penalty which, in case of a data fiduciary may extend to twenty thousand rupees for each day during which such default continues, subject to a maximum of two crore rupees, and in case of a data processor may extend to five thousand rupees for each day during which such default continues, subject to a maximum of fifty lakh rupees.

73. Penalty for contravention where no separate penalty has been provided.—

Where any person fails to comply with any provision of this Act, or rules prescribed or regulations specified thereunder as applicable to such person, for which no separate penalty has been provided, then such person shall be liable to a penalty subject to a maximum of one crore rupees in case of significant data fiduciaries, and a maximum of twenty five lakh rupees in all other cases.

74. Adjudication by Adjudicating Officer.—

- (1) No penalty shall be imposed under this Chapter except after conducting an inquiry in such manner as may be prescribed, and the data fiduciary or data processor or any person, as the case may be, has been given a reasonable opportunity of being heard.
- (2) While holding an inquiry, the Adjudicating Officer shall have the power to summon and enforce the attendance of any person acquainted with the facts and circumstances of the case to give evidence or to produce any document which, in the opinion of the Adjudicating Officer, may be useful for or relevant to the subject matter of the inquiry.
- (3) If, on the conclusion of such inquiry, the Adjudicating Officer is satisfied that the person has failed to comply with the provisions of this Act or has caused harm to any data principal as a result of any violation of the provisions of this Act, which a penalty may be imposed under section 69 to section 73, the Adjudicating Officer may impose a penalty in accordance with the provisions of the appropriate section.
- (4) While deciding whether to impose a penalty under sub-section (3) of this section and in determining the quantum of penalty under section 69 to section 73, the Adjudicating Officer shall have due regard to the following factors, as may be applicable —
 - (a) nature, gravity and duration of violation taking into account the nature, scope and purpose of processing concerned;
 - (b) number of data principals affected, and the level of harm suffered by them;
 - (c) intentional or negligent character of the violation;
 - (d) nature of personal data impacted by the violation;
 - (e) repetitive nature of the default;

- (f) transparency and accountability measures implemented by the data fiduciary or data processor including adherence to any relevant code of practice relating to security safeguards;
 - (g) action taken by the data fiduciary or data processor to mitigate the harm suffered by data principals; and
 - (h) any other aggravating or mitigating factors relevant to the circumstances of the case, such as, the amount of disproportionate gain or unfair advantage, wherever quantifiable, made as a result of the default.
- (5) Any person aggrieved by an order under this section by the Adjudicating Officer may prefer an appeal to the Appellate Tribunal.

75. Compensation.—

- (1) Any data principal who has suffered harm as a result of any violation of any provision under this Act, or rules prescribed or regulations specified hereunder, 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.

Explanation.- For the removal of doubts, it is hereby clarified that a data processor shall be liable only where it has acted outside or contrary to the instructions of the data fiduciary pursuant to section 37, or where the data processor is found to have acted in a negligent manner, or where the data processor has not incorporated adequate security safeguards under section 31, or where it has violated any provisions of this Act expressly applicable to it.

- (2) The data principal may seek compensation under this section pursuant to a complaint instituted in such form and manner as may be prescribed before an Adjudicating Officer.
- (3) Where there are one or more data principals or any identifiable class of data principals who have suffered harm as a result of any violation by the same data fiduciary or data processor, one complaint may be instituted on behalf of all such principals seeking compensation for the harm suffered.
- (4) While deciding whether to award compensation and the amount of compensation under this section, the Adjudicating Officer shall have due regard to the following factors, namely—
 - (a) nature, duration and extent of violation of the provisions of the Act, rules prescribed, or regulations specified thereunder;
 - (b) nature and extent of harm suffered by the data principal;
 - (c) intentional or negligent character of the violation;
 - (d) transparency and accountability measures implemented by the data fiduciary or the data processor, as the case may be, including adherence to any relevant code of practice relating to security safeguards;
 - (e) action taken by the data fiduciary or the data processor, as the case may be, to mitigate the damage suffered by the data principal;

- (f) previous history of any, or such, violation by the data fiduciary or the data processor, as the case may be;
 - (g) whether the arrangement between the data fiduciary and data processor contains adequate transparency and accountability measures to safeguard the personal data being processed by the data processor on behalf of the data fiduciary;
 - (h) any other aggravating or mitigating factor relevant to the circumstances of the case, such as, the amount of disproportionate gain or unfair advantage, wherever quantifiable, made as a result of the default.
- (5) Where more than one data fiduciary or data processor, or both a data fiduciary and a data processor are involved in the same processing activity and are found to have caused harm to the data principal as per this section, then each data fiduciary or data processor may be ordered to pay the entire compensation for the harm in order to ensure effective and speedy compensation to the data principal.
- (6) Where a data fiduciary or a data processor has, in accordance with sub-section (5), paid the entire amount of compensation for the harm suffered by the data principal, such data fiduciary or data processor shall be entitled to claim from the other data fiduciaries or data processors, as the case may be, that amount of compensation corresponding to their part of responsibility for the harm caused.
- (7) Any person aggrieved by an order made under this section by the Adjudicating Officer may prefer an appeal to the Appellate Tribunal.
- (8) The Central Government may prescribe the procedure for hearing of a complaint under this section.

76. Compensation or penalties not to interfere with other punishment.—

No compensation awarded, or penalty imposed, under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force.

77. Data Protection Funds.—

- (1) There shall be constituted a fund to be called the Data Protection Authority Fund to which the following shall be credited—
- (a) all Government grants, fees and charges received by the Authority under this Act; and
 - (b) all sums received by the Authority from such other source as may be decided upon by the Central Government, but which shall not include the sums mentioned in sub-section (3).
- (c) 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 and for the purposes of this Act.
- (2) 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.
- (3) The Data Protection Awareness Fund shall be applied solely for the purpose of generating awareness regarding data protection including for the purposes set out in clauses (m), (o) and (p) of sub-section (2) of section 61 and for no other purpose whatsoever.

78. Recovery of Amounts.—

- (1) The Authority shall, by an order in writing, appoint at least one officer or employee as a Recovery Officer for the purpose of this Act.
- (2) Where any person fails to comply with—
 - (a) an order of the Adjudicating Officer imposing a penalty under the provisions of this Act; or
 - (b) an order of the Adjudicating Officer directing payment of compensation under the provisions of this Act,

the Recovery Officer may recover from such person the aforesaid amount in any of the following ways, in descending order of priority, namely—

- (i) attachment and sale of the person's movable property;
 - (ii) attachment of the person's bank accounts;
 - (iii) attachment and sale of the person's immovable property;
 - (iv) arrest and detention of the person in prison;
 - (v) appointing a receiver for the management of the person's movable and immovable properties.
- (3) For the purpose of such recovery, the provisions of section 220 to section 227, and sections 228A, 229 and 232, the Second and Third Schedules of the Income Tax Act, 1961 (43 of 1961) and the Income Tax (Certificate Proceedings) Rules, 1962, as in force from time to time, in so far as may be, shall apply with necessary modifications as if the said provisions and rules—
- (a) were the provisions of this Act; and
 - (b) referred to the amount due under this Act instead of to income tax under the Income Tax Act, 1961 (43 of 1961).
- (4) In this section, the movable or immovable property or monies held in a bank account shall include property or monies which meet all the following conditions—

- (a) property or monies transferred by the person without adequate consideration;
 - (b) such transfer is made:
 - (i) on or after the date on which the amount in the certificate drawn up under section 222 of the Income Tax Act, 1961 (43 of 1961) had become due; and
 - (ii) to the person's spouse, minor child, son's wife or son's minor child.
 - (c) such property or monies are held by, or stand in the name of, any of the persons referred to in sub-clause (b), including where they are so held or stand in the name of such persons after they have attained the age of majority.
- (5) The Recovery Officer shall be empowered to seek the assistance of the local district administration while exercising the powers under this section.

CHAPTER XII

APPELLATE TRIBUNAL

79. Establishment of Appellate Tribunal.—

- (1) The Central Government shall, by notification, establish an Appellate Tribunal to—
 - (a) hear and dispose of any appeal from an order of the Adjudicating Officer under sub-section (5) of section 39;
 - (b) hear and dispose of any appeal from an order of the Authority under sub-section (2) of section 65;
 - (c) hear and dispose of an application under sub-section (9) of section 66;
 - (d) hear and dispose of any appeal from an order of the Adjudicating Officer under sub-section (5) of section 74; and
 - (e) hear and dispose of any appeal from an order of an Adjudicating Officer under sub-section (7) of section 75.
- (2) The Appellate Tribunal shall consist of a chairperson and such number of members as may be notified by the Central Government.
- (3) The Appellate Tribunal shall be set up at such place or places, as the Central Government may, in consultation with the chairperson of the Appellate Tribunal, notify.
- (4) Where, in the opinion of the Central Government, any existing body is competent to discharge the functions of the Appellate Tribunal as envisaged under this Act, then the Central Government may notify such existing body to act as the Appellate Tribunal under this Act.

80. Qualifications, appointment, term, conditions of service of members.—

- (1) The Central Government may prescribe the qualifications, appointment, term of office, salaries and allowances, resignation, removal and the other terms and conditions of service of the chairperson and any member of the Appellate Tribunal.
- (2) Neither the salary and allowances nor the other terms and conditions of service of the chairperson or member of the Appellate Tribunal may be varied to her disadvantage after her appointment.

81. Vacancies.—

If, for reason other than temporary absence, any vacancy occurs in the office of the chairperson or a member of the Appellate Tribunal, the Central Government shall appoint another person in accordance with the provisions of this Act and the rules prescribed to fill the vacancy and the proceedings may be continued before the Appellate Tribunal from the stage at which the vacancy is filled.

82. Staff of Appellate Tribunal.—

- (1) The Central Government shall provide the Appellate Tribunal with such officers and employees as it may deem fit.
- (2) The officers and employees of the Appellate Tribunal shall discharge their functions under the general superintendence of its chairperson.
- (3) The salaries and allowances and other conditions of service of such officers and employees of the Appellate Tribunal shall be such as may be prescribed.

83. Distribution of business amongst benches.—

- (1) Subject to the provisions of this Act, the jurisdiction of the Appellate Tribunal may be exercised by benches thereof, which shall be constituted by the chairperson.
- (2) Where benches of the Appellate Tribunal are constituted under sub-section (1), the chairperson may, from time to time, by notification, make provisions as to the distribution of the business of the Appellate Tribunal amongst the benches, transfer of members between benches, and also provide for the matters which may be dealt with by each bench.
- (3) On the application of any of the parties and after notice to the parties, and after hearing such of them as the chairperson may desire to be heard, or on the chairperson's own motion without such notice, the chairperson of the Appellate Tribunal may transfer any case pending before one bench, for disposal, to any other bench.

84. Appeals to Appellate Tribunal.—

- (1) Any person may file an appeal or application, as the case may be, with the Appellate Tribunal in such form, verified in such manner and be accompanied by such fee, as may be prescribed.
- (2) Any appeal or application to the Appellate Tribunal, as the case may be, shall be preferred within a period of thirty days from the date on which a copy of the decision or order made by the Authority or the Adjudicating Officer, as the case may be, is received by the appellant or applicant and it shall be in such form, verified in such manner and be accompanied by such fee as may be prescribed.
- (3) Notwithstanding sub-section (2), the Appellate Tribunal may entertain any appeal or application, as the case may be, after the expiry of the said period of thirty days if it is satisfied that there was sufficient cause for not filing it within that period.
- (4) On receipt of an appeal or application, as the case may be, under this section, the Appellate Tribunal may, after providing the parties to the dispute or appeal, an opportunity of being heard, pass such orders thereon as it thinks fit.
- (5) The Appellate Tribunal shall send a copy of every order made by it to the parties to the dispute or the appeal and to the Authority, as the case may be.
- (6) The Appellate Tribunal may, for the purpose of examining the legality or propriety or correctness, of any decision, or order of the Authority or Adjudicating Officer referred to in the appeal or application preferred under this section, on its own motion or otherwise, call for the records relevant to disposing of such appeal or application and make such orders as it thinks fit.

85. Procedure and powers of Appellate Tribunal.—

- (1) The Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908), but shall be guided by the principles of natural justice and, subject to the other provisions of this Act, the Appellate Tribunal shall have powers to regulate its own procedure.
- (2) The Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely—
 - (a) summoning and enforcing the attendance of any person and examining her on oath;
 - (b) requiring the discovery and production of documents;
 - (c) receiving evidence on affidavits;
 - (d) subject to the provisions of section 123 and section 124 of the Indian Evidence Act, 1872 (1 of 1872), requisitioning any public record or document or a copy of such record or document, from any office;

- (e) issuing commissions for the examination of witnesses or documents;
 - (f) reviewing its decisions;
 - (g) dismissing an application for default or deciding it, *ex parte*;
 - (h) setting aside any order of dismissal of any application for default or any order passed by it, *ex parte*; and
 - (i) any other matter which may be prescribed.
- (3) Every proceeding before the Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code, 1860 (45 of 1860) and the Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973 (2 of 1974).

86. Orders passed by Appellate Tribunal to be executable as a decree.—

- (1) An order passed by the Appellate Tribunal under this Act shall be executable by the Appellate Tribunal as a decree of civil court, and for this purpose, the Appellate Tribunal shall have all the powers of a civil court.
- (2) Notwithstanding anything contained in sub-section (1), the Appellate Tribunal may transmit any order made by it to a civil court having local jurisdiction and such civil court shall execute the order as if it were a decree made by that court.

87. Appeal to Supreme Court of India.—

- (1) Notwithstanding anything contained in the Code of Civil Procedure, 1908 (5 of 1908) or in any other law, an appeal shall lie against any order of the Appellate Tribunal to the Supreme Court of India.
- (2) No appeal shall lie against any decision or order made by the Appellate Tribunal with the consent of the parties.
- (3) Every appeal under this section shall be preferred within a period of ninety days from the date of the decision or order appealed against.
- (4) Notwithstanding sub-section (3), the Supreme Court of India may entertain the appeal after the expiry of the said period of ninety days, if it is satisfied that the appellant was prevented by sufficient cause from preferring the appeal in time.

88. Right to legal representation.—

The applicant or appellant may either appear in person or authorise one or more legal practitioners or any of its officers to present her or its case before the Appellate Tribunal.

Explanation.- For the purposes of this section, "legal practitioner" includes an advocate, or an attorney and includes a pleader in practice.

89. Civil court not to have jurisdiction.—

No civil court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which the Appellate Tribunal is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

**CHAPTER XIII
OFFENCES**

90. Obtaining, transferring or selling of personal data contrary to the Act.—

Any person who alone or jointly with others, knowingly or intentionally or recklessly, in contravention of the provisions of this Act—

- (a) obtains personal data; or
- (b) discloses personal data; or
- (c) transfers personal data to another person; or
- (d) sells or offers to sell personal data to another person,

which results in significant harm to a data principal, then such person shall be punishable with imprisonment for a term not exceeding three years or shall be liable to a fine which may extend up to rupees two lakh or both.

91. Obtaining, transferring or selling of sensitive personal data contrary to the Act.—

Any person who alone or jointly with others, knowingly or intentionally or recklessly, in contravention of the provisions of this Act—

- (a) obtains sensitive personal data; or
- (b) discloses sensitive personal data; or
- (c) transfers sensitive personal data to another person; or
- (d) sells or offers to sell sensitive personal data to another person,

which results in harm to a data principal, then such person 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.

92. Re-identification and processing of de-identified personal data.—

- (1) Any person who, knowingly or intentionally or recklessly—
 - (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 shall be liable to a fine which may extend up to rupees two lakh or both.

- (2) Nothing contained in sub-section (1) shall render any such person liable to any punishment provided under this section, if she proves that—
 - (a) the personal data belongs to the person charged with the offence under sub-section (1); or
 - (b) the data principal whose personal data is in question has explicitly consented to such re-identification or processing as per the provisions of this Act.

93. Offences to be cognizable and non-bailable.—

Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), an offence punishable under this Act shall be cognizable and non-bailable.

94. Power to investigate offences.—

Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of Inspector shall investigate any offence under this Act.

95. Offences by companies.—

- (1) Where an offence under this Act has been committed by a company, every person who, at the time the offence was committed was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company, shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.
- (2) Nothing contained in sub-section (1) shall render any such person liable to any punishment provided in this Act, if she proves that the offence was committed without

her knowledge or that she had exercised all due diligence to prevent the commission of such offence.

- (3) Notwithstanding anything contained in sub-section (1), where an offence under this Act has been committed by a company and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

Explanation.- For the purpose of this section—

- (a) “company” means any body corporate, and includes—
 - (i) a firm; and
 - (ii) an association of persons or a body of individuals whether incorporated or not.
- (b) “director” in relation to—
 - (i) a firm, means a partner in the firm;
 - (ii) an association of persons or a body of individuals, means any member controlling affairs thereof.

96. Offences by Central or State Government departments. —

- (1) Where an offence under this Act has been committed by any department of the Central or State Government, or any authority of the State, the head of the department or authority shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.
- (2) Nothing contained in sub-section (1) shall render any such person liable to any punishment provided in this Act, if she proves that the offence was committed without her knowledge or that she had exercised all due diligence to prevent the commission of such offence.
- (3) Notwithstanding anything contained in sub-section (1), where an offence under this Act has been committed by a department of the Central or State Government, or any authority of the State and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any neglect on the part of, any officer, other than the head of the department or authority, such officer shall also be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

CHAPTER XIV
TRANSITIONAL PROVISIONS

97. Transitional provisions and commencement. —

- (1) For the purposes of this Chapter, the term ‘notified date’ refers to the date notified by the Central Government under sub-section (3) of section 1.
- (2) The notified date shall be any date within twelve months from the date of enactment of this Act.
- (3) The following provisions shall come into force on the notified date—
 - (a) Chapter X;
 - (b) Section 107; and
 - (c) Section 108.
- (4) The Central Government shall, no later than three months from the notified date establish the Authority.
- (5) The Authority, shall, no later than twelve months from the notified date, notify the grounds of processing personal data in respect of the activities listed in sub-section (2) of section 17.
- (6) The Authority, shall, no later than twelve months from the notified date issue codes of practice on the following matters—
 - (a) notice under section 8;
 - (b) data quality under section 9;
 - (c) storage limitation under section 10;
 - (d) processing of personal data under Chapter III;
 - (e) processing of sensitive personal data under Chapter IV;
 - (f) security safeguards under section 31;
 - (g) research purposes under section 45;
 - (h) exercise of data principal rights under Chapter VI;
 - (i) methods of de-identification and anonymisation; and
 - (j) transparency and accountability measures under chapter VII.
- (7) Section 40 shall come into force on such date as is notified by the Central Government for the purpose of that section.
- (8) The remaining provisions of the Act shall come into force eighteen months from the notified date.

CHAPTER XV

MISCELLANEOUS

98. Power of Central Government to issue directions in certain circumstances. —

- (1) The Central Government may, from time to time, issue to the Authority such directions as it may think necessary in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order.
- (2) Without prejudice to the foregoing provisions of this Act, the Authority shall, in exercise of its powers or the performance of its functions under this Act, be bound by such directions on questions of policy as the Central Government may give in writing to it from time to time:
- (3) Any direction issued by the Central Government shall, as far as practicable, be given, after providing an opportunity to the Authority to express its views in this regard.
- (4) The decision of the Central Government on whether a question is one of policy or not, shall be final.

99. Members, etc., to be public servants. —

The chairperson, members, officers and employees of the Authority and the Appellate Tribunal shall be deemed, when acting or purporting to act in pursuance of any of the provisions of this Act, to be public servants within the meaning of section 21 of the Indian Penal Code, 1860 (45 of 1860).

100. Protection of action taken in good faith. —

No suit, prosecution or other legal proceedings shall lie against the Authority or its chairperson, member, employee or officer for anything which is done in good faith or intended to be done under this Act, or the rules prescribed, or the regulations specified thereunder.

101. Exemption from tax on income. —

Notwithstanding anything contained in the Income Tax Act, 1961 (43 of 1961) or any other enactment for the time being in force relating to tax on income, profits or gains, as the case may be, the Authority shall not be liable to pay income tax or any other tax in respect of its income, profits or gains derived.

102. Delegation. —

The chairperson of the Authority may, by general or special order in writing delegate to any member or officer of the Authority subject to such conditions, if any, as may be specified in the order, such of its powers and functions under this Act except the powers under section 108 as it may deem necessary.

103. Power to remove difficulties.—

- (1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order, published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to be necessary or expedient for removing the difficulty.
- (2) No such order shall be made under this section after the expiry of five years from the commencement of this Act.
- (3) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

104. Power to exempt certain data processors.—

The Central Government may, by notification, exempt from the application of this Act or any provisions of this Act, processing of personal data of data principals not within the territory of India, pursuant to any contract entered into with any person outside the territory of India, including any company incorporated outside the territory of India, by any data processor or any class of data processors incorporated under Indian law.

105. No application to non-personal data

Nothing contained in this Act shall affect the power of the Central Government to formulate appropriate policies for the digital economy, including measures for its growth, security, integrity, prevention of misuse, insofar as such policies do not govern personal data.

106. Bar on processing certain forms of biometric data

No data fiduciary shall process such biometric data as may be notified by the Central Government, unless such processing is permitted by law.

107. Power to make rules. —

- (1) The Central Government may, by notification, make rules to carry out the purposes of this Act.
- (2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely—
 - (a) the form and manner in which an application to exercise the right under sub-section (4) of Section 27;
 - (b) the manner of review of the order passed by the Adjudicating Officer under sub-section (5) of section 27;
 - (c) the manner in which a complaint with the adjudication wing may be filed under sub-section (4) of section 39;

- (d) the countries, sectors within a country, or international organisations to which transfers may be permitted under clause (b) of sub-section (1) of section 41;
- (e) the time period of notification to the Authority under sub-section (4) of section 41 of the transfer of personal data to a particular country as permitted under clause (b) of sub-section (3) of section 41;
- (f) the amount of turnover for a data fiduciary to qualify as a small entity under clause (a) of sub-section (2) of section 48;
- (g) the place of establishment and incorporation of the head office of the Authority as under sub-section (3) of section 49;
- (h) procedure to be followed by the selection committeeunder sub-section (3) of section 50;
- (i) the salaries and allowances payable to, and other terms and conditions of service of the chairperson and the members of the Authority under sub-section (2) of section 51;
- (j) the times and places for, and the rules and procedures in regard to, transaction of business at the meetings of the Authority under sub-section (1) of section 54;
- (k) the form of accounts, other relevant records and annual statement of accounts under sub-section (1) of section 58;
- (l) the intervals at which the accounts of the Authority will be audited under sub-section (2) of section 58;
- (m) the time in which, and the form and manner in whichthe returns, statements, and particulars are to be furnished to the Central Government under sub-section (1) of section 59;
- (n) the time in which, and the form in which an annual report is to be prepared by the Authority and forwarded to the Central Government under sub-section (2) of section 59;
- (o) other functions of the Authority under clause (x) of sub-section (2) of section 60;
- (p) other matters under clause (e) of sub-section (3) of section 60 in respect of which the Authority shall have powers under the Code of Civil Procedure, 1908 (5 of 1908) that are vested in a civil court while trying a suit;
- (q) the procedure of issuance of a code of practice under sub-section (4) of section 61;
- (r) the manner in which the Authority may review, modify or revoke a code of practice under sub-section (9) of section 61;
- (s) the manner in which the Authority shall maintain a register containing details of the codes of practice under sub-section (10) of section 61;
- (t) the process for search and seizure under sub-section (11) of section 66;
- (u) the number of Adjudicating Officers that the adjudication wing will consist of under sub-section (2) of section 68;
- (v) the qualification, manner and terms of appointment, and jurisdiction of Adjudicating Officers to ensure their independence, and the procedure for carrying out adjudication under this Act and other such requirements as deemed fit by the Central Government under sub-section (2) of section 68;
- (w) the manner in which the Adjudicating Officer will conduct an inquiry under sub-section (1) of section 74;
- (x) the form and manner of instituting a complaint under sub-section (2) of section 75;
- (y) the procedure for hearing of a complaint and the limit on the amount of compensation under sub-section (8) of section 75;

- (z) the qualifications, appointment, term of office, salaries and allowances, resignation, removal and the other terms and conditions of service of the chairperson and any member of the Appellate Tribunal under sub-section (1) of section 80;
- (aa) the procedure of filling of vacancies in the Appellate Tribunal under section 81;
- (bb) the salaries and allowances and other conditions of service of the officers and employees of the Appellate Tribunal under sub-section (3) of section 82;
- (cc) the form, manner and fee for filing an appeal or application, as the case may be, with the Appellate Tribunal under sub-section (1) of section 84; and
- (dd) other matters under clause (i) of sub-section (2) of section 85 in respect of which the Appellate Tribunal shall have powers under the Code of Civil Procedure, 1908 (5 of 1908) that are vested in a civil court while trying a suit.

108. Power to make regulations. —

- (1) The Authority may, by notification, make regulations consistent with this Act and the rules prescribed thereunder to carry out the purposes 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, namely:
 - (a) information required to be provided by the data fiduciary to the data principal in its notice under clause (n) of sub-section (1) of section 8;
 - (b) manner in which the personal data retained by the data fiduciary must be deleted under sub-section (4) of section 10;
 - (c) reasonable purposes for which personal data may be processed in accordance with sub-section (2) of section 17;
 - (d) safeguards as may be appropriate for protecting the rights of data principals under sub-section (3) of section 17;
 - (e) any further categories of sensitive personal data and further grounds on which such data may be processed under sub-section (1) of section 22;
 - (f) such additional safeguards or restrictions applicable to processing of sensitive personal data and any further categories of personal data where there is repeated, continuous, systematic collection for the purposes of profiling and such additional safeguards required under sub-section (3) of section 22;
 - (g) the additional factors necessary for determining the appropriateness of age verification mechanisms to be incorporated by a data fiduciary processing the personal data and sensitive personal data of children under sub-section (3) of section 23;
 - (h) practices that may be undertaken by data fiduciaries offering counseling or child protection services under sub-section (6) of section 23;
 - (i) the time period within which a data fiduciary must comply with a request made under sub-section (3) of section 28;
 - (j) the time period within which a data principal may file a complaint under sub-section (4) of section 28;
 - (k) the form in which the data fiduciary is required to make available to the data principal information under sub-section (1) of section 30;

- (l) the manner by which a data fiduciary shall notify the data principal regarding important operations in the processing of personal data under sub-section (2) of section 30;
- (m) the manner of periodic review of security safeguards to be undertaken by the data fiduciary and the data processor under sub-section (2) of section 31;
- (n) the circumstances or classes of data fiduciaries or processing operations where it is mandatory to carry out data protection impact assessments under sub-section (2) of section 33;
- (o) the instances where a data auditor under this Act shall be engaged by the data fiduciary to undertake a data protection impact assessment under sub-section (2) of section 33;
- (p) the manner in which the data fiduciary shall submit the data protection impact assessment to the Authority under sub-section (4) of section 33;
- (q) any aspect of processing for which records shall be maintained under clause (d) of sub-section (1) of section 34;
- (r) the form in which records shall be maintained under sub-section (2) of section 34;
- (s) the factors to be taken into consideration while evaluating the compliance of data fiduciaries with the provisions of this Act under sub-section (2) of section 35;
- (t) the form, manner and procedure by which data audits shall be conducted under sub-section (3) of section 35;
- (u) criteria on the basis of which rating in the form of a data trust score may be assigned to a data fiduciary under sub-section (6) of section 35;
- (v) the eligibility, qualifications and functions to be performed by data auditors under sub-section (4) of section 35;
- (w) the eligibility and qualification of a data protection officer under sub-section (3) of section 36;
- (x) the registration requirements of significant data fiduciaries under sub-section (2) of section 38;
- (y) the manner of certification and time period within which transfer of personal data shall be notified to the Authority under sub-section (6) of section 41;
- (z) the provisions of the Act which may be exempted for different categories of research, archival or statistical purposes under sub-section (1) of section 45;
- (aa) the remuneration, salary or allowances and other terms and conditions of service of such officers, employees, consultants and experts under sub-section (2) of section 56;
- (bb) any other fees and charges for carrying out purposes of this Act under clause (t) of sub-section (2) of Section 60;
- (cc) the manner in which information shall be provided to the authority by the data fiduciary under sub-section (3) of Section 63; and
- (dd) any other matter which is required to be, or may be specified, or in respect of which provision is to be or may be made by regulations.

109. Rules and Regulations to be laid before Parliament.—

Every rule and regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately

following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or regulation or, both Houses agree that the rule or regulation should not be made, the rule or regulation shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule or regulation.

110. Overriding effect of this Act. —

Save as otherwise expressly provided under this Act, the provisions of this Act shall have an overriding effect to the extent that such provisions are inconsistent with any other law for the time being in force or any instrument having effect by virtue of any such law.

111. Amendment of Act 21 of 2000. —

The Information Technology Act, 2000 (21 of 2000) shall be amended in the manner set out in the First Schedule to this Act.

112. Amendment of Act 22 of 2005. —

The Right to Information Act, 2005 (22 of 2005) shall be in the manner set out in the Second Schedule to this Act.

THE FIRST SCHEDULE
(See Section 111)
AMENDMENT TO THE INFORMATION TECHNOLOGY ACT, 2000
(21 of 2000)

- 1. Deletion of section 43A.** — Section 43A of the Information Technology Act, 2000 (hereinafter referred to as the principal Act) shall be omitted.
- 2. Amendment of section 87.** — In section 87 of the principal Act, in sub-section (2), clause (ob) shall be omitted.

THE SECOND SCHEDULE
(SEE SECTION 112)
AMENDMENT TO THE RIGHT TO INFORMATION ACT, 2005
(22 OF 2005)

1. Amendment of section 8. — In place of the current clause (j) of sub-section (1) of section 8 of the Right to Information Act, 2005 the following clause (j) of sub-section (1) of section 8 shall be substituted, namely:—

“(j) information which relates to personal data which is likely to cause harm to a data principal, where such harm outweighs the public interest in accessing such information having due regard to the common good of promoting transparency and accountability in the functioning of the public authority;

Provided, disclosure of information under this clause shall be notwithstanding anything contained in the Personal Data Protection Act, 2018;

Provided further, that the information, which cannot be denied to the Parliament or a State Legislature shall not be denied to any person.

Explanation. —For the purpose of this section, the terms ‘personal data’, ‘data principal’, and ‘harm’ shall have the meaning assigned to these terms in the Personal Data Protection Act, 2018.”

A Free and Fair Digital Economy

Protecting Privacy, Empowering Indians

**Committee of Experts under the Chairmanship of Justice B.N.
Srikrishna**

TABLE OF CONTENTS

GLOSSARY OF TERMS.....	1
CHAPTER 1: A FREE AND FAIR DIGITAL ECONOMY.....	3
A. Existing Approaches to Data Protection.....	3
B. Understanding the Contours of the Indian Approach.....	4
C. Data Principles and Data Fiduciaries.....	7
D. Following Puttaswamy	10
E. Chapters in the Report	11
F. Methodology	13
G. Summary: A Fourth Way to Privacy, Autonomy and Empowerment.....	13
CHAPTER 2: JURISDICTION AND APPLICABILITY.....	15
A. White Paper and Public Comments	15
B. Analysis	16
I. Jurisdiction.....	16
(a) Conceptual Understanding of Jurisdiction	16
(b) Prescriptive Jurisdiction	17
(c) The Case for Data Non-Exceptionalism.....	18
(d) Putative Bases for Jurisdiction	18
II. Retrospective and Transitional Application of the Data Protection Law	21
RECOMMENDATIONS	23
CHAPTER 3: PROCESSING	24
A. White Paper and Public Comments	24
B. Analysis	27
I. Building Blocks of the Law.....	27
(a) Personal Data.....	27
(b) Sensitive Personal Data	30
II. Consent	32
(a) A revised operational framework for consent	33
(b) Consequences of such a Framework	34
(c) Enforcement of the Revised Framework.....	35
(d) Standard of Consent	36
(e) Different Standards for Different Types of Personal Data Processing	37
(f) Consent Dashboard and Avoiding Consent Fatigue.....	38
(g) Consent and Contractual Necessity	40
III. Protection of Children's Personal Data	42
(a) Identification of guardian data fiduciaries.....	43
(b) Who is a child?	43
(c) Barred Practices.....	44
(d) Regulatory Approach	44
IV. Community Data.....	45
V. Entities to which the Law Applies.....	46

RECOMMENDATIONS	48
CHAPTER 4: OBLIGATIONS OF DATA FIDUCIARIES	49
A. White Paper and Public Comments	49
B. Analysis	51
I. Fair and Reasonable Processing	51
II. Purpose Limitation and Data Minimisation.....	52
III. Big Data Challenges to Data Minimisation and Purpose Limitation	54
IV. Transparency	58
V. Organisational Obligations on Data Fiduciaries.....	59
VI. Storage Limitation	60
VII. Data Quality.....	62
VIII. Notification for Data Breach	62
(a) Need for Data Breach Notification.....	62
(b) What constitutes a Personal Data Breach?	63
(c) When does it need to be notified to the DPA?	64
(d) When does it need to be notified to individuals?	64
IX. Data Security	65
RECOMMENDATIONS	67
CHAPTER 5: DATA PRINCIPAL RIGHTS	68
A. Access, Confirmation and Correction	68
I. White Paper and Public Comments	68
II. Analysis	69
B. Rights to Objection, Restriction and Portability.....	71
I. White Paper and Public Comments	72
II. Analysis	73
C. The Right to be Forgotten.....	75
I. White Paper and Public Comments	76
II. Analysis	77
(a) Balancing the Right with Competing Rights and Interests	78
(b) Appropriate Entity for the Approval of Requests	79
(c) Breadth of Application of Orders	80
RECOMMENDATIONS	81
CHAPTER 6: TRANSFER OF PERSONAL DATA OUTSIDE INDIA.....	82
A. White Paper and Public Comments	82
B. Analysis	83
I. Cross-Border Transfer of Personal Data	83
II. Exceptions to Free Transfer of Personal Data Outside India	87

(a) Benefits.....	88
(b) Costs	93
RECOMMENDATIONS	97
CHAPTER 7: ALLIED LAWS	98
A. Impact on Allied Laws	98
B. Amendments to the Aadhaar Act.....	98
C. Amendments to the RTI Act.....	102
RECOMMENDATIONS	105
CHAPTER 8: NON-CONSENSUAL PROCESSING	106
Non-Consensual Grounds for Processing	107
A. White Paper and Public Comments	107
B. Analysis	107
I. Functions of the State	108
(a) Context	108
(b) Scope	110
(c) Application of Obligations	112
II. Compliance with Law or Order of Court or Tribunal	112
(a) Context	112
(b) Scope	113
(c) Application of Obligations	113
III. Prompt Action.....	114
(a) Context	114
(b) Scope	115
(c) Application of Obligations	115
IV. Employment.....	115
(a) Context	115
(b) Scope	116
(c) Application of Obligations	116
V. Reasonable Purpose.....	117
(a) Context	117
(b) Scope	117
(c) Application of Obligations	120
Exemptions	120
A. White Paper and Public Comments	120
B. Analysis	121
I. Security of the State.....	122
(a) Context	122
(b) Scope	128
(c) Application of Obligations	129
II. Prevention, Detection, Investigation and Prosecution of Contraventions of Law....	129
(a) Context	129

(b)	Scope	133
(c)	Application of Obligations	134
III.	Processing for the purpose of legal proceedings	135
(a)	Context	135
(b)	Scope	136
(c)	Application of Obligations	136
IV.	Research Activities	136
(a)	Context	136
(b)	Scope	137
(c)	Application of Obligations	138
V.	Personal or Domestic Purposes	139
(a)	Context	139
(b)	Scope	141
(c)	Application of Obligations	141
VI.	Journalistic Activities	142
(a)	Context	142
(i)	Conflict between Privacy and Free Speech	142
(ii)	Ethics Standards	144
(b)	Scope	145
(c)	Application of Obligations	146
VII.	Manual Processing by Small Entities	147
(a)	Context	147
(b)	Scope	148
(c)	Application of Obligations	148
RECOMMENDATIONS	149	
CHAPTER 9: ENFORCEMENT	151	
A.	The Data Protection Authority: Structure, Functions and Tools	151
I.	White Paper and Public Comments	151
II.	Analysis	152
(a)	Structure and Functions of the DPA.....	152
(i)	Establishment.....	152
(ii)	Composition.....	153
(iii)	Functions of the DPA	153
(b)	Enforcement Tools	156
(i)	Issuance of a Direction	156
(ii)	Power to call for Information	156
(iii)	Publication of Guidance	157
(iv)	Issuance of a Public Statement	157

(v)	Codes of Practice	157
(vi)	Conducting Inquiries	158
(vii)	Injunctive Relief	158
(viii)	Inter-sectoral coordination.....	158
(c)	Adjudication Wing of the DPA	158
(d)	Appellate Tribunal.....	159
B.	The Regulated Entities: Classification and Obligations	159
I.	White Paper and Public Comments	159
II.	Analysis	160
(a)	Significant Data Fiduciaries	160
(i)	Registration	161
(ii)	Data Protection Impact Assessment	161
(iii)	Record-keeping	161
(iv)	Data Audits.....	162
(v)	Data Protection Officer	163
C.	Penalties, Compensation and Offences	163
I.	White Paper and Public Comments	163
II.	Analysis	164
(a)	Burden of Proof and Accountability	164
(b)	Penalties.....	164
(c)	Compensation.....	165
(d)	Offences.....	165
RECOMMENDATIONS		166
SUMMARY OF RECOMMENDATIONS.....		166
ANNEXURES		
APPENDIX		

GLOSSARY OF TERMS

S. No.	Defined Term	Definition
1.	Aadhaar Act	The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016
2.	AI	Artificial Intelligence
3.	ALRC	Australian Law Reform Commission
4.	ALRC Report	For Your Information: Australian Privacy Law and Practice (Australian Law Reform Commission Report 108).
5.	CAG	Comptroller and Auditor General of India
6.	CCI	Competition Commission of India
7.	CLOUD Act	The Clarifying Lawful Overseas Use of Data Act, 2018 (US)
8.	Committee	Committee of Experts on a Data Protection Framework for India under the chairmanship of (retd.) Justice B.N. Srikrishna
9.	Competition Act	Competition Act, 2002
10.	Contract Act	The Indian Contract Act, 1872
11.	COPPA	Children's Online Privacy Protection Act, 1998 (US)
12.	CRC	United Nations Convention on the Rights of the Child
13.	CrPC	Code of Criminal Procedure, 1973
14.	CVC	Central Vigilance Commission
15.	Cyber Security Law of China	People's Republic of China Cyber Security Law of 2016
16.	Data Protection Directive of 1995	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
17.	DPIA	Data Protection Impact Assessment
18.	DPO	Data Protection Officer
19.	DPA	Data Protection Authority
20.	EEA	European Economic Area
21.	EU	European Union
22.	EU GDPR	European Union General Data Protection Regulation
23.	FIPP	Fair Information Practice Principles
24.	FISA	Foreign Intelligence Surveillance Act, 1978 (US)
25.	FISC	Foreign Intelligence Surveillance Court
26.	FTC	Federal Trade Commission
27.	GDP	Gross Domestic Product
28.	GLB Act	Gramm Leach Bliley Act (US)

29.	Income Tax Act	Income Tax Act, 1961
30.	Investigatory Powers Act, 2016	Investigatory Powers Act (UK)
31.	IRDA Act	Insurance and Regulatory Authority of India Act, 1999
32.	IT Act	Information Technology Act, 2000
33.	MLAT	Mutual Legal Assistance Treaty
34.	NATGRID	National Intelligence Grid
35.	NETRA	Network Traffic Analysis
36.	NIA Act	National Investigation Agency Act, 2008
37.	OECD	Organisation for Economic Cooperation and Development
38.	PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 2001 (US)
39.	PMLA	Prevention of Money Laundering Act, 2002
40.	POPI Act	Protection of Personal Information Act, 2013 (South Africa)
41.	RBI	Reserve Bank of India
42.	RTI Act	Right to Information Act, 2005
43.	SEBI	Securities and Exchange Board of India
44.	SEBI Act	Securities and Exchange Board of India Act, 1992
45.	SPD Rules	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
46.	Telegraph Act	The Indian Telegraph Act, 1885
47.	Telegraph Rules	Indian Telegraph Rules, 1951
48.	TOR	Terms of Reference of the Committee
49.	TRAI	Telecom Regulatory Authority of India
50.	TRAI Act	Telecom Regulatory Authority of India Act, 1997
51.	UK	United Kingdom
52.	UK DPA	The Data Protection Act, 1998
53.	UK Data Protection Bill	Data Protection Bill [HL] 2017-19
54.	US	United States of America

CHAPTER 1: A FREE AND FAIR DIGITAL ECONOMY

This report is based on the fundamental belief shared by the entire Committee that if India is to shape the global digital landscape in the 21st century, it must formulate a legal framework relating to personal data that can work as a template for the developing world. Implicit in such a belief is the recognition that the protection of personal data holds the key to empowerment, progress, and innovation. Equally implicit is the need to devise a legal framework relating to personal data not only for India, but for Indians.

Such a framework must understand from the ground up the particular concerns and aspirations pertaining to personal data shared by Indians, their fears and hopes. It is a platitude that such viewpoints may not necessarily be the same in developed countries, which already have established legal frameworks. The report thus ploughs its own furrow, responding to the challenges that India faces as a developing nation in the Global South. At the same time, it adopts learnings from best practices that exist in developed democracies with considerably advanced thinking on the subject.

A. Existing Approaches to Data Protection

In today's world, broadly three approaches to data protection exist. The US follows a *laissez-faire* approach and does not have an overarching data protection framework. US courts however, have collectively recognised a right to privacy by piecing together the limited privacy protections reflected in the First, Fourth, Fifth and Fourteenth Amendments to the US Constitution.¹ Consequently, certain legislation, the Privacy Act, 1974, the Electronic Communications Privacy Act, 1986 and the Right to Financial Privacy Act, 1978 protect citizens against the federal government. With regard to the private sector, while no omnibus legislation exists, it has sector-specific laws that have carefully tailored rules for specific types of personal data. For example, the GLB Act² has well-defined provisions for collection and use of financial data.³

The EU, at the vanguard of global data protection norms has recently enacted the EU GDPR, which has come into force on 25 May 2018. This replaces the Data Protection Directive of 1995. It is a comprehensive legal framework that deals with all kinds of processing of personal data while delineating rights and obligations of parties in detail. It is both technology and sector-agnostic and lays down the fundamental norms to protect the privacy of Europeans, in all its facets. We are informed that 67 out of 120 countries outside Europe largely adopt this framework or that of its predecessor.⁴

¹ Roe v. Wade 410 U.S. 113 (1973); Griswold v. Connecticut 381 U.S. 479 (1965). See Ryan Moshell, And Then There Was One: The Outlook For A Self-Regulatory United States Amidst A Global Trend Towards Comprehensive Data Protection, 37 Texas Tech Law Review (2005).

² The GLB Act is also known as The Financial Services Modernization Act of 1999.

³ A noted data protection scholar, Graham Greenleaf has argued in his submission that the US approach cannot be called a 'model' since no other country follows it. See comments in response to the White Paper submitted by Graham Greenleaf on 31 January 2018, available on file with the Committee at p. 4.

⁴ Comments in response to the White Paper submitted by Graham Greenleaf on 31 January 2018, available on file with the Committee at p. 4.

Though the aforementioned approaches have dominated global thinking on the subject, recently, China has articulated its own views in this regard. It has approached the issue of data protection primarily from the perspective of averting national security risks. Its cybersecurity law, which came into effect in 2017,⁵ contains top-level principles for handling personal data. A follow-up standard (akin to a regulation) issued earlier this year adopts a consent-based framework with strict controls on cross-border sharing of personal data.⁶ It remains to be seen how such a standard will be implemented.

Each of these regimes is founded on each jurisdiction's own understanding of the relationship between the citizen and the state in general, and the function of the data protection law, in particular.⁷ In the US, the *laissez-faire* approach to regulating data handling by private entities while imposing stringent obligations on the state is based on its constitutional understanding of liberty as freedom from state control.⁸ Data protection is thus an obligation primarily on the state and certain categories of data handlers who process data that are considered worthy of public law protection. In Europe on the other hand, data protection norms are founded on the need to uphold individual dignity.⁹ Central to dignity is the privacy of the individual by which the individual herself determines how her personal data is to be collected, shared or used with anyone, public or private. The state is viewed as having a responsibility to protect such individual interest. China, on the other hand, frames its law with the interests of the collective as the focus, based on its own privileging of the collective over the individual.

B. Understanding the Contours of the Indian Approach

Each of these legal regimes described above has acceptability in its respective jurisdiction because it captures the zeitgeist of the citizen-state relationship that exists in each. At the

⁵ Cyber Security Law of China.

⁶ Standard number: GB/T 35273-2017 available at <<http://www.gb688.cn/bzgk/gb/newGbInfo?hcno=4FFAA51D63BA21B9EE40C51DD3CC40BE>> (last accessed on 20 April 2018).

Further, see Samm Sacks, New China Data Privacy Standard Looks More Far-reaching than EU GDPR, Centre for Strategic and International Studies (2018) available at <<https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr>> (last accessed on 20 April 2018).

⁷ For an insightful account on cultural bases for privacy protections, see James Q. Whitman, The Two Western Cultures of Privacy: Dignity Versus Liberty, 113 Yale Law Journal 1151 (2004).

⁸ This derives from the American Declaration of Independence, 1776 a charter of limited government. "We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights that among these are Life, Liberty and the pursuit of Happiness. That to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed, That whenever any Form of Government becomes destructive of these ends, it is the Right of the People to alter or to abolish it, and to institute new Government, laying its foundation on such principles and organising its powers in such forms, as to them shall seem most likely to affect their Safety and Happiness."

⁹ This is succinctly stated in the Census Act Judgment of the German Constitutional Court on 15 December, 1983 recognising a right to informational self-determination.

"From this follows that free development of personality presupposes, in the context of modern data processing, protection of individuals against the unrestricted collection, storage, use and transfer of their personal data. This protection is therefore subsumed under the fundamental right contained in Article 2.1 in conjunction with Article 1.1 of the Basic Law ("human dignity shall be inviolable")."

Unofficial translation available at <<https://freiheitsfoo.de/census-act/>> (last accessed on 9 May 2018).

same time, it is trite that neither is India's understanding of its citizen-state relationship, nor its motivations for a data protection law, exactly coincident with each of the aforementioned jurisdictions. The conceptualisation of the state in the Constitution is based on two planks — first, the state is a facilitator of human progress. Consequently, it is commanded by the Constitution in Part IV (Directive Principles of State Policy) to serve the common good;¹⁰ second, the state is prone to excess. Hence it is checked by effectuating both a vertical (federal structure) and horizontal (three organs of government) separation of powers, as well as by investing every individual with fundamental rights that can be enforced against the state.

The right to privacy has been recently recognised as a fundamental right emerging primarily from Article 21 of the Constitution, in *Justice K.S. Puttaswamy (Retd.) v. Union of India*.¹¹ To make this right meaningful, it is the duty of the state to put in place a data protection framework which, while protecting citizens from dangers to informational privacy originating from state and non-state actors, serves the common good. It is this understanding of the state's duty that the Committee must work with while creating a data protection framework.

The TORs (annexed in **Annexure A**) mandate both a study of various data protection related issues in India along with specific suggestions for a data protection framework and a draft bill. This must be seen in light of the objective of the Government of India in setting up of the Committee, also contained in the TORs, “to unlock the data economy, while keeping data of citizens secure and protected.” This objective appears to be based on the salient realisation that data has the potential to both empower as well as to harm.

The transformative potential of the digital economy to improve lives in India and elsewhere, is seemingly limitless at this time. Artificial Intelligence holds out the promise of new breakthroughs in medical research¹² and Big Data generates more calibrated searches and allows quicker detection of crime.¹³ Large-scale data analytics allows machines to discern patterns and constantly improves services in an endless virtual loop. The prospects of such data gathering and analysis to benefit citizens is immense.

¹⁰ Specifically, Article 39(b) and (c) of the Constitution direct the state to make policy towards securing distributed ownership and control of material resources and preventing concentration of wealth to common detriment.

¹¹ 2017 (10) SCALE 1.

¹² The use of AI in the health industry in India is well documented. For instance, in the context of hospitals the Manipal Hospital Group has partnered with IBM's Watson for Oncology for the diagnosis and treatment of seven types of cancer, while in the context of pharmaceuticals, AI software is being used for scanning through all available academic literature for tasks such as molecule discovery. For further details and more instances of the use of AI in healthcare see E. Hickok et al, Artificial Intelligence in the Healthcare Industry in India, The Centre for Internet and Society, India (undated) available at <<https://cis-india.org/internet-governance/files/ai-and-healthcare-report>> (last accessed on 19 April 2018).

¹³ For predictive policing, see Rohan George, Predictive Policing: What is it, How it works, and its Legal Implications, The Centre for Internet and Society, India (24 November 2015) available at <<https://cis-india.org/internet-governance/blog/predictive-policing-what-is-it-how-it-works-and-its-legal-implications>> (last accessed on 20 April 2018); For details on the potential of data analytics for the detection of money laundering see, Business Today (12 October 2016) available at <<https://www.businesstoday.in/current/economy-politics/how-big-data-and-analytics-can-help-india-fight-against-money-laundering/story/238397.html>> (last accessed on 19 April 2018).

At the same time, the potential for discrimination, exclusion and harm is equally likely in a digital economy. The recent admission by Facebook that the data of 87 million users, including 5 lakh Indian users, was shared with Cambridge Analytica through a third-party application that extracted personal data of Facebook users who had downloaded the application as well as their friends, is demonstrative of several such harms - users did not have effective control over data. Further, they had little knowledge that their activity on Facebook would be shared with third parties for targeted advertisements around the US elections. The incident, unfortunately is neither singular, nor exceptional. Data gathering practices are usually opaque, mired in complex privacy forms that are unintelligible, thus leading to practices that users have little control over. Inadequate information on data flows and consequent spam or worse still, more tangible harms,¹⁴ are an unfortunate reality. Equally, the state collects and processes significant amounts of personal data of citizens, with much of such processing being related to its functions. Despite the fact that the State is able to exercise substantial coercive power, and despite ambiguous claims to personal data that may not be necessary for its functions, the State remains largely unregulated on this account.

Currently, the law does little to protect individuals against such harms in India. The transfer of personal data (defined as “sensitive personal data or information”) is governed by the SPD Rules.

The SPD Rules were issued under Section 43A of the IT Act which holds a body corporate liable for compensation for any negligence in implementing and maintaining reasonable security practices and procedures while dealing with sensitive personal data or information. The SPD Rules expand on the scope of these reasonable practices and procedures. They define sensitive personal data¹⁵ and mandate the implementation of a policy for dealing with such data.¹⁶ Further, various conditions such as consent requirement,¹⁷ lawful purpose,¹⁸ purpose limitation,¹⁹ subsequent withdrawal of consent,²⁰ etc., have been imposed on the body corporate collecting such information.

¹⁴ In July 2017 it was reported that important personal information including social security numbers, birth dates, addresses, and in some cases drivers' license numbers, credit card numbers of around 147.9 million US citizens were breached due to the outdated technological safeguards used by the credit information company Equifax; See Equifax's Massive 2017 Data Breach Keeps Getting Worse, The Washington Post (1 March 2018) available at <https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach/?noredirect=on&utm_term=.03e306802d4e> (last accessed on 19 April 2018); In 2016 data from more than 412.2 million accounts on the Friend Finder's Network was breached by hackers due to weak data security protections, See Adult Friend Finder and Penthouse hacked in massive personal data breach, The Guardian (14 November 2016) available at <<https://www.theguardian.com/technology/2016/nov/14/adult-friend-finder-and-penthouse-hacked-in-largest-personal-data-breach-on-record>> (last accessed on 19 April 2018); In India, in early 2017 it was reported that personal information from McDonald's delivery app was leaked due to inadequate security features, See McDonald's India delivery app ‘leaks users data’, BBC News (20 March 2017) available at <<http://www.bbc.com/news/technology-39265282>> (last accessed on 19 April 2018).

¹⁵ Rule 3, SPD Rules.

¹⁶ Rule 4, SPD Rules.

¹⁷ Rule 5(1), SPD Rules.

¹⁸ Rule 5(2), SPD Rules.

¹⁹ Rules 5(4) and (5), SPD Rules.

The SPD Rules require the prior consent of the provider of the information while disclosing sensitive personal data to a third party.²¹ Transfer of sensitive personal data outside India is permitted on the condition that the same level of data protection is adhered to in the country, which is applicable to the body corporate under the SPD Rules.²² The body corporate would further be deemed to have complied with reasonable security practices if it has complied with security standards and has comprehensive data security policies in place.²³

While the SPD Rules were a novel attempt at data protection at the time they were introduced, the pace of development of the digital economy has made it inevitable that some shortcomings have become apparent over time. For instance, the definition of sensitive personal data is unduly narrow, leaving out several categories of personal data from its protective remit;²⁴ its obligations do not apply to the government and may, on a strict reading of Section 43A of the IT Act be overridden by contract. The IT Act and SPD Rules have also suffered from problems of implementation due to delays in appointments to the adjudicatory mechanisms created under the IT Act.²⁵ Some of these are not peculiarly Indian problems but endemic in several jurisdictions.

The deficiencies in regulation of data flows in India (and elsewhere in the world) is a consequence of a simplistic assumption that data flows are an unadulterated good. This is only partially accurate. It is clear that several data flows can cause considerable harm. But more significantly, the treatment of free data flows as an intrinsic good, as the recent exposé of data sharing practices by Facebook demonstrates, has placed the interests of the individual in whose name the information flows, as secondary to the interests of companies of various kinds which deal with the data. This gives a different complexion to the terminology in various jurisdictions designating the individual whose data is being collected as the “**data subject**” and the entity that collects the data as the “**data controller**”. We begin by revisiting this terminology.

C. Data Principals and Data Fiduciaries

It is our view that any regime that is serious about safeguarding personal data of the individual must aspire to the common public good of both a free and fair digital economy.²⁶ Here, freedom refers to enhancing the autonomy of the individuals with regard to their personal data in deciding its processing which would lead to an ease of flow of personal data.

²⁰ Rule 5(7), SPD Rules.

²¹ Rule 6, SPD Rules.

²² Rule 7, SPD Rules.

²³ Rule 8, SPD Rules.

²⁴ Graham Greenleaf, India – Confusion Raj with Outsourcing in Asian Data Privacy Laws: Trade and Human Rights Perspectives (Oxford University Press, 2017) at p. 415.

²⁵ Sreenidhi Srinivasan and Namrata Mukherjee, Building an effective data protection regime, Vidhi Centre for Legal Policy, New Delhi (2017) at pp. 18-19.

²⁶ Arghya Sengupta, Facebook’s Brave New World, The Times of India (9 April 2018) available at: <https://blogs.timesofindia.indiatimes.com/toi-edit-page/facebook-s-brave-new-world-india-needs-strong-rules-to-ensure-internet-is-not-only-free-but-also-fair/> (last accessed on 17 May 2018).

Fairness pertains to developing a regulatory framework where the rights of the individual with respect to her personal data are respected and the existing inequality in bargaining power between individuals and entities that process such personal data is mitigated. In such a framework, the individual must be the “***data principal***” since she is the focal actor in the digital economy. The relationship between the individual and entities with whom the individual shares her personal data is one that is based on a fundamental expectation of trust. Notwithstanding any contractual relationship, an individual expects that her personal data will be used fairly, in a manner that fulfils her interest and is reasonably foreseeable. This is the hallmark of a fiduciary relationship.²⁷ In the digital economy, depending on the nature of data that is shared, the purpose of such sharing and the entities with which sharing happens, data principals expect varying levels of trust and loyalty. For entities, this translates to a duty of care to deal with such data fairly and responsibly for purposes reasonably expected by the principals. This makes such entities “***data fiduciaries***”.²⁸

Pursuant to this, and as a general canon, data fiduciaries must only be allowed to share and use personal data to fulfil the expectations of the data principal in a manner that furthers the common public good of a free and fair digital economy. It is our considered view that a regime based on the principles mentioned above and implemented through the relations described above will ensure individual autonomy and make available the benefits of data flows to the economy, as mandated by the TOR.

The twin objectives of protecting personal data while unlocking the data economy have often been seen as conflicting with each other.²⁹ Specifically, the TOR which mandates both these objectives, is said to have set up a false choice between societal interests and individual interests, a trade-off between economic growth and data protection.³⁰ It is argued that both are designed to achieve the constitutional objectives of individual autonomy, dignity and self-determination.

In our view, ensuring the protection of personal data and facilitating the growth of the digital economy are not in conflict and has rightly been pointed out, serve a common constitutional objective. However, each of them is motivated by distinct intermediate rationales — the former ensuring the protection of individual autonomy and consequent harm prevention and the latter seeking to create real choices for citizens. Both these intermediate objectives themselves are complementary — individual autonomy becomes truly meaningful when real choice (and not simply an illusory notion of it) can be exercised and likewise no real choice is possible if individuals remain vulnerable. The growth of the digital economy, which is

²⁷ Tamar Frankel, Fiduciary Law, 71(3) California Law Review (1983) at p. 795.

²⁸ This is taken from the view expressed by Jack M. Balkin, Jack M Balkin, Information Fiduciaries and the First Amendment, 49(4) UC Davis Law Review (2016) at p.1183.

²⁹ Elina Pyykkö, Data Protection at the cost of economic growth?, European Credit Research Institute, ECRI Commentary No. 11 (November 2012) available at <<https://www.ceps.eu/system/files/ECRI%20Commentary%20No%2011%20Data%20protection.pdf>> (last accessed on 20 April 2018).

³⁰ See Submission by legal academics and advocates to the Justice Srikrishna Committee of Experts on Data Protection (31 January 2018) available at <<http://privacyisaright.in/wp-content/uploads/2018/02/Detailed-Answers-to-the-Justice-Srikrishna-Committee-White-Paper-1.pdf>> (last accessed on 20 April 2018).

proceeding apace worldwide, must be equitable, rights-reinforcing and empowering for the citizenry as a whole. In this, to see the individual as an atomised unit, standing apart from the collective, neither flows from our constitutional framework nor accurately grasps the true nature of rights litigation.

Rights (of which the right to privacy is an example) are not deontological categories that protect interests of atomised individuals;³¹ on the contrary, they are tools that as Raz points out, are necessary for the realisation of certain common goods.³² The importance of a right in this account is not because of the benefit that accrues to the rights holder but rather because that benefit is a public good that society as a whole enjoys. This is a critical distinction, and often missed in simplistic individual-centric accounts of rights.

This is an argument made most forcefully by Richard Pildes.³³ Pildes provides an example — in *Pico v. United States*,³⁴ the question before the US Supreme Court was whether a decision by a school to ban certain books from the library on account of them being “anti-American, anti-Christian, anti-Semitic and just plain filthy” violated the right to free speech of the students under the First Amendment. The decision to strike down the ban, Pildes believes, is justified not because the free speech right — in this case to receive information freely — is weightier than the state interest in promoting certain values in public education. Were this the case, it would be difficult to trammel the right to receive information freely at all. On the contrary, it was justified because the school could not remove books on the basis of hostility to the ideas that they contained — such reasons were illegitimate in this context where the common good is a public education system that differentiates politics from education. A decision on rights is thus a decision on the justifiability of state action in a given context that is necessary to serve the common good.

Thus the construction of a right itself is not because it translates into an individual good, be it autonomy, speech, etc. but because such good creates a collective culture where certain reasons for state action are unacceptable. In the context of personal data collection, use and sharing in the digital economy, it is our view that protecting the autonomy of an individual is critical not simply for her own sake but because such autonomy is constitutive of the common good of a free and fair digital economy. Such an economy envisages a polity where the individual is autonomously deciding what to do with her personal data, entities are responsibly sharing such data and everyone is using data, which has immense potential for empowerment, in a manner that promotes overall welfare.

³¹ Ronald Dworkin, an influential legal philosopher, argues that rights of individuals against the state exist outside the framework of state sanctioned rights and act as trumps against the imposition of majoritarian decision-making. For details, see R. Dworkin, *Taking Rights Seriously* (Harvard University Press, 1978). The applicability of such a theoretical framework to actual constitutional practice is questionable. See Joseph Raz, *Rights and Individual Well-Being*, in *Ethics in the Public Domain: Essays in the Morality of Law and Politics* (Clarendon, 1995).

³² Joseph Raz, *Rights and Individual Well-Being*, 5(2) *Ratio Juris* (1992) at p. 127.

³³ See R. Pildes, *Why rights are not trumps: social meanings, expressive harms, and constitutionalism*, 27(2) *The Journal of Legal Studies* (1998) at pp. 725-763.

³⁴ 69 U.S. 279 (1864).

Thus keeping citizens' personal data protected while unlocking the digital economy, as the TOR mandates, are both necessary. This will protect individual autonomy and privacy which can be achieved within the rubric of a free and fair digital economy. This is the normative framework that India, as a developing nation needs to assuredly chart its course in the increasingly digital 21st century.

D. Following Puttaswamy

This normative foundation of the proposed data protection framework is true to the ratio of the judgment of the Supreme Court of India in *Puttaswamy*.³⁵ The Supreme Court held that the right to privacy is a fundamental right flowing from the right to life and personal liberty as well as other fundamental rights securing individual liberty in the Constitution. In addition, individual dignity was also cited as a basis for the right. Privacy itself was held to have a negative aspect, (the right to be let alone), and a positive aspect, (the right to self-development).³⁶ The sphere of privacy includes a right to protect one's identity. This right recognises the fact that all information about a person is fundamentally her own, and she is free to communicate or retain it for herself.³⁷ This core of informational privacy, thus, is a right to autonomy and self-determination in respect of one's personal data. Undoubtedly, this must be the primary value that any data protection framework serves.

However, there may be other interests to consider, on which, the Court observed as follows:

*"Formulation of a regime for data protection is a complex exercise which needs to be undertaken by the State after a careful balancing of the requirements of privacy coupled with other values which the protection of data sub-serves together with the legitimate concerns of the State."*³⁸

Thus, like other fundamental rights, privacy too can be restricted in well-defined circumstances. For such a restriction, three conditions need to be satisfied: first, there is a legitimate state interest in restricting the right; second, that the restriction is necessary and proportionate to achieve the interest; third that the restriction is by law.³⁹ As the excerpt from *Puttaswamy* above establishes, two points are critical — first, the primary value that any data protection framework serves must be that of privacy; second, such a framework must not overlook other values including collective values. In our view, the normative framework of a free and fair digital economy can provide a useful reference point for balancing these values in a particular case. To understand whether in a certain case, a right to privacy over that which is claimed exists, and would prevail over any legitimate interests of the state would depend on the interpretation by courts on how the needs of a free and fair digital economy

³⁵ 2017 (10) SCALE 1.

³⁶ See Bert-Jaap Koops et al., A Typology of Privacy, 38(2) University of Pennsylvania Journal of International Law (2017) at p. 566, as cited by Chandrachud, J., in *Puttaswamy*, (2017) 10 SCALE 1 at para 141.

³⁷ Her Majesty, The Queen v. Brandon Roy Dyment (1988) 2 SCR 417 as cited in *Puttaswamy* (2017) 10 SCALE 1.

³⁸ Per Chandrachud, J., in *Puttaswamy*, (2017) 10 SCALE 1 at para 179.

³⁹ Per Chandrachud, J., in *Puttaswamy*, (2017) 10 SCALE 1 at para 180.

can be best protected. It may happen by fully upholding the right, or alternatively finding the restriction justified, or a partial application of one or the other. The normative framework for this exercise is provided by the values of freedom and fairness. After all, freedom and fairness are the cornerstones of our constitutional framework, the *raison d'être* of our struggle for independence.

E. Chapters in the Report

In order to ensure that a free and fair digital economy is a reality in India, there is certainly a need for a law that protects personal data. This report sets the framework for the contents of such a law and this could further be instrumental in shaping the discourse on data protection in the Global South.

Chapter 2 is a discussion of fundamental questions relating to scope and applicability of such a law. The question of scope of data protection laws in different jurisdictions is vexed — seamless transferability of data across national boundaries, has, for some, eroded the importance of the nation state.⁴⁰ While the factual premise of seamless transferability is largely correct, absent a global regulatory framework, national legislations supported by well-established conflicts of laws rules will govern issues relating to jurisdiction over personal data. In a legislation for India, questions of scope and applicability must be answered according to our policy objective of securing a free and fair digital economy. This objective will be severely compromised if data of Indians is processed, whether in India or elsewhere, without complying with our substantive obligations. Implicit in this is the ability of the state to hold parties accountable, irrespective of where data might have been transferred, and particularly to be able to enforce such obligations against errant parties. At the same time this objective cannot be enforced in derogation of established rules of international comity, respecting the sovereignty of other jurisdictions in enforcing its own rules.

Chapter 3 deals with the processing of personal data. Consistent with our view that the digital economy should be free and fair, the autonomy of the individual whose data is the lifeblood of this economy should be protected. Thus, a primary basis for processing of personal data must be individual consent. This recommendation is not oblivious to the failings of the consent framework. Consent is often uninformed, not meaningful and operates in an all-or-nothing fashion. This chapter provides an alternate framework of consent that treats the consent form, not as a means to an end, but rather as an end in itself. This imposes form and substance obligations on entities seeking consent as well as more effective mechanisms for individuals to track and withdraw consent.

Chapters 4 and 5 deal with obligations on data fiduciaries and rights of data principals. Anyone who uses personal data has an obligation to use it fairly and responsibly. This is the cardinal tenet of the proposed framework. We envisage the DPA and courts developing this principle on a case-by-case basis over time ensuring robust protection for individual data. At

⁴⁰ Jennifer Daskal, *The Un-territoriality of Data*, 125 Yale Law Journal (2015) at p. 326.

the same time, certain substantive obligations are critical if the objective of a free and fair digital economy is to be met. Specifically, these obligations ensure that the data principal is aware of the uses to which personal data is put and create bright line rules on when personal data can be collected and stored by data fiduciaries. This segues into Chapter 5 which deals with the rights of data principals. This is consistent with the principle that if the data principal is the entity who legitimises data flows, she must continue to exercise clearly delineated rights over such data. The scope of such rights, their limitations and their methods of enforcement are discussed in detail.

The flow of data across borders is essential for a free and fair digital economy. However, such flows cannot be unfettered, and certain obligations need to be imposed on data fiduciaries who wish to transfer personal data outside India. At the same time India's national interests may require local storage and processing of personal data. This has been dealt with in Chapter 6.

Chapter 7 discusses the impact of the proposed data protection framework on all allied laws which may either set a different standard for the protection of privacy or might otherwise authorise or mandate the processing of large amounts of personal data. Particularly, the impact on and necessary amendments to the IT Act, the Aadhaar Act and the RTI Act are discussed.

There are situations where rights and obligations of data principals and data fiduciaries may not apply in totality. This manifests in limited instances where consent may not be used for processing to serve a larger public interest such as 'national security', 'prevention and investigation of crime', 'allocation of resources for human development', 'protection of the revenue'. These have been recognised in *Puttaswamy* as legitimate interests of state. A discussion of such grounds where consent may not be relevant for processing is contained in Chapter 8. While some of the situations listed here only allow for processing without consent (non-consensual grounds), others are situations where substantive obligations of the law apply partially (exemptions). A critical element of this discussion relates to the safeguards governing such processing in order to prevent their wrongful use. Specific safeguards for both the grounds and the partial exemptions to the law are thus delineated together with the obligations that would continue to apply, notwithstanding such derogation from consent.

Critical to the efficacy of any legal framework is its enforcement machinery. This is especially significant in India's legal system, which has often been characterised as long on prescriptions and short on enforcement. This requires careful redressal. To achieve this, enforcement of this law must be conceived as having both an internal and an external element. External enforcement requires the establishment of an authority, sufficiently empowered and adequately staffed to administer data protection norms in India. However, we are cognizant of the limitations of a single authority to enforce a law of such significant magnitude, irrespective of whether it has nation-wide presence and resources. Consequently, any internal aspect of enforcement implies the need to formulate a clear legislative policy on *ex ante* organisational measures. Such policy and measures are to be enforced by codes of

practice to be developed in consultation with sectoral regulators, regulated entities and data principals, through an open and participatory process. Chapter 9 contains the details of the enforcement machinery under the proposed framework.

The report concludes with a summary of recommendations that we would urge the Government of India to adopt expeditiously in the form of a data protection law. A suggested draft of such a law has been provided along with this report.

F. Methodology

While framing the report, the Committee has conducted wide consultations. A White Paper was published by the Committee on 27 November 2017 for public comments. In addition, four public consultations were conducted by the Committee in New Delhi on 5 January 2018, Hyderabad on 12 January 2018, Bengaluru on 13 January 2018, and Mumbai on 23 January 2018. A number of views were expressed both in the written comments submitted to the Committee as well as oral representations at the public consultations. As will be evident from this report, such views, together with further research, have significantly informed our work, often departing from tentative viewpoints that may have been presented in the White Paper. This demonstrates the participatory and deliberative approach followed by the Committee in the task before it.

We are cognisant of the limitations of this report and lay no claims to exhaustiveness. The digital economy is a vast and dynamic space and we have consciously avoided wading into territories that do not strictly come within the framework of data protection issues set out in our TOR. Needless to say, such issues will have to be gone into at the appropriate time if our framework of a free and fair digital economy is to be truly upheld. Notably, these issues include those of intermediary liability, effective enforcement of cyber security and larger philosophical questions around the citizen-state relationship in the digital economy, all of which have been raised in public comments and committee meetings. Our deliberations have also raised questions related to non-personal data and emerging processing activities that hold considerable strategic or economic interest for the nation. Data processing is equally linked to the creation of useful knowledge, impinging values such as reliability, assurance and integrity. Many issues related to electronic communications infrastructure and services also arise in the larger context of the digital economy.⁴¹ We leave such questions to the wisdom of a future committee in the hope that they will be duly considered.

G. Summary: A Fourth Way to Privacy, Autonomy and Empowerment

In our view, a combination of the elements outlined above would deliver a personal data protection law that protects individual privacy, ensures autonomy, allows data flows for a growing data ecosystem and creates a free and fair digital economy. In other words, it sets the

⁴¹ See, for instance, UK Digital Economy Act 2017 (dealing with issues such as digital government, age verification and filters, universal service obligations related to internet speed, nuisance calls, copyright infringements and public service broadcasters).

foundations for a growing, digital India that is at home in the 21st century. This is distinct from the approaches in the US, EU and China and represents a fourth path. This path is not only relevant to India, but to all countries in the Global South which are looking to establish or alter their data protection laws in light of the rapid developments to the digital economy. After all, the proposition that the framework is based on is simple, commanding itself to universal acceptability — a free and fair digital economy that empowers the citizen can only grow on the foundation of individual autonomy, working towards maximising the common good.

CHAPTER 2: JURISDICTION AND APPLICABILITY

Questions regarding scope and applicability are critical to any law, since they determine the extent of coverage of its rights and obligations. The issue of jurisdiction is the starting point since it answers two fundamental questions: first, whose interest the state seeks to uphold; second, why it is relevant for the state to uphold such interest. In the context of data protection, the borderless nature of the internet has challenged conventional views on jurisdiction and has often necessitated some form of extra-territorial application.

Every new law comes into force by intervening into existing practices, legal rules and conditions in a jurisdiction. For the effective implementation of the new rules, it is important to clarify the temporal applicability of the proposed framework as well as any provisions that allow for a smooth transition. As a result of these considerations, the chapter also deals with the issue of retrospective and transitional operation of any prospective data protection law.

A. White Paper and Public Comments

With respect to jurisdiction, the provisional view taken in the White Paper was to cover all instances of processing of personal data in the territory of India by entities having a presence in India.⁴² With many companies not being based in India but carrying on business, or offering goods or services in India, it was also felt that the state had a legitimate interest in regulating such processing activities not entirely based in India or carried out by non-Indian entities that do not have a presence in India.⁴³ The Committee considered it worthwhile to extend the law to all entities processing the personal data of Indian citizens or residents; however it was felt that the law should not encroach upon the jurisdiction of other states which may have the effect of making the law a general law of the internet.⁴⁴

A majority of the commenters were in favour of the law having some form of extra-territorial application. Covering foreign entities which deal with the data of Indian residents was stressed upon as necessary to ensure effective protection. However, the extent of such protection was varying with some suggesting expansive coverage, while others limited it to the formulation in the EU GDPR (i.e., entities offering goods and services in India). The commenters who argued against extra-territoriality did so largely on the basis of the impracticability of having to comply with competing obligations. As an alternative to extra-territorial application, a co-regulation model was suggested.⁴⁵

⁴² White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 28.

⁴³ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 28.

⁴⁴ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 28.

⁴⁵ Comments in response to the White Paper submitted by Aditya Kutty of Uber India Systems Private Limited on 31 January 2018, available on file with the Committee.

On the further issue of the applicability of the law, transitional provisions were suggested in the White Paper to address the issue of retrospective application for ongoing processing.⁴⁶ Commenters largely agreed with this suggestion.

B. Analysis

I. Jurisdiction

(a) Conceptual Understanding of Jurisdiction

As is evident from the public responses, the scope of application of the proposed data protection law throws up several questions of principle and implementation. These questions are not unique to data protection — the nature of the internet as a seamless cross-jurisdictional network of accessible switches and pipes means that traditional concepts of territorial jurisdiction may require a rethink. This encompasses both substantive reassessment of the meaning of territoriality, as well as a careful calibration of any extra-territorial application of a prospective law in concert with principles of international comity. In this process, the two principled objectives that must guide Indian thinking on the issue of application of the data protection law are as follows:

- (i) Need to protect the personal data of persons present in India;⁴⁷
- (ii) Instituting a fair compliance mechanism for data fiduciaries who might operate in multiple jurisdictions; and
- (iii) Establishing a domestic model that can be replicated by other jurisdictions such that each respects international comity.

Fortunately, this is not a greenfield subject. Legal scholars have, for a considerable period of time, debated the very same questions in the context of trying to understand the concept of jurisdiction. At its core, ‘jurisdiction’ is an exercise of power to define rights and obligations of parties.⁴⁸ Practically, the exercise of this power takes three forms — prescriptive, enforcement and adjudicatory.⁴⁹ Prescriptive jurisdiction refers to the power to make a law applicable to parties; enforcement jurisdiction is the supplementary power to enforce the law on the pain of penalty against parties; and adjudicatory jurisdiction is the power to judge the

⁴⁶ White Paper of the Committee of Experts on a Data Protection Framework for India available at http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf (last accessed on 20 April 2018) at p. 32.

⁴⁷ For example, in the EU data subjects who are “in the Union” are accorded protection, see Article 3(2) and Recital 23, EU GDPR.

⁴⁸ Arthur T. von Mehren and Donald T. Trautman, Jurisdiction to Adjudicate: A Suggested Analysis, 79(6) Harvard Law Review (1966) at p. 1126.

⁴⁹ See Andrew Keane Woods, Against Data Exceptionalism, 68 Stanford Law Review (2016) at pp. 765-773; See also Jack Goldsmith, Unilateral Regulation of the Internet: A modest defence, 11(1) European Journal of International Law (2000) at p. 139.

actions of parties, consequently determining rights and obligations.⁵⁰ At this stage, our interest is limited to the question of prescriptive jurisdiction alone, i.e., defining the legitimate scope of legislative power.

(b) Prescriptive Jurisdiction

Prescriptive jurisdiction has been understood in a seminal publication as capable of being exercised on five grounds:⁵¹

- (i) Territoriality: Territorial jurisdiction is based on the occurrence of the cause of action within the borders of the state seeking to exercise jurisdiction over it. It is the fundamental public policy of each state to regulate actions in its territory based on the principle that any action that takes place in the territory, or any company that enjoys the benefits of the territory in carrying on business must be amenable to its legal framework.
- (ii) Nationality: The nationality principle is based on the nationality of the alleged actor whose conduct has been called into question. The nationality principle is justified by the sovereign's interest in retaining control over the acts of its nationals wherever they may be.
- (iii) Protective: The protective principle relies on the concept that a country should be able to protect its interests against acts abroad that have transnational effects. It requires jurisdiction to be vested to protect a security interest or the operation of the country's governmental functions, irrespective of where such interest lies.
- (iv) Universality: The universality principle is based on the concept that all nations have an interest in combating certain trans-border crimes, such as piracy, slave trading, hijacking, etc.
- (v) Passive Personality: The principle of passive personality permits a country to exercise jurisdiction over an act committed by an individual outside its territory because the victim is one of that country's nationals.

Related bases include objective territoriality and the effects doctrine,⁵² wherein though acts might have been committed outside the territory of the state, they either have been completed in the state or have significant effects on the state thereby warranting the exercise of jurisdiction.⁵³

⁵⁰ Arthur T. von Mehren and Donald T. Trautman, *Jurisdiction to Adjudicate: A Suggested Analysis*, 79(6) Harvard Law Review (1966) at p. 1125; A. Benjamin Spencer, *Jurisdiction to Adjudicate: A Revised Analysis*, 73 University of Chicago Law Review (2006) at p. 617; Adria Allen, *Internet Jurisdiction Today*, 22(1) Northwestern Journal of International Law & Business (2001) at p. 75.

⁵¹ *Jurisdiction with Respect to Crime*, 29 American Journal of International Law (1935) at p. 519 (this was in the context of criminal law where several cross-jurisdictional questions were raised).

⁵² *Banyan Tree Holding v. Murali Krishna* 2010(42)PTC 361.

⁵³ Christopher Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part 1)*, 18(2) International Journal of Law and Information Technology (2010) at p. 20.

(c) The Case for Data Non-Exceptionalism

It has been argued by several authors that data is un-territorial and thus traditional bases of jurisdiction described above are not easily applicable.⁵⁴ By virtue of being mobile, divisible, partitioned and location-independent, the nature of data challenges territoriality as the basis for exercise of jurisdiction.

This case for data exceptionalism has been questioned on various counts. First, any intangible asset such as intellectual property or debt has similar features to data in terms of being mobile (capable of being transferred or moved to offshore accounts) and divisible (in terms of being physically divided).⁵⁵ The law has established rules of jurisdiction for dealing with such assets. Second, data is not really as location-independent as it is posited to be. Even data on the cloud, actually physically resides on a server that is in the territory of a nation-state.⁵⁶ Once reduced to its physical form, exercise of jurisdiction appears to become a less complex exercise.

Third, much prior to the digital age, the possibility of transnational effects of domestic acts and *vice versa* were not unknown to the legal system. A decree against a defendant in one jurisdiction might lead to attachment of his properties in other jurisdictions if such property exists and none exists in the jurisdiction where the decree was passed. Similarly, regulations on trawlers by one country would affect the trawler no matter where it fishes. Neither of these actions prevents unilateral regulation by one state.⁵⁷ In the event that more than one state can exercise jurisdiction, a conflict-of-laws situation emerges, and courts will determine which country has the more ‘substantial connection’ to exercise jurisdiction. Similarly, for data which may not reside in one jurisdiction alone, an assessment of jurisdiction must be made in light of traditional principles that apply when an action has connections with multiple jurisdictions. It is not exceptional in terms of requiring a fundamental rethink of traditional legal formulations.

(d) Putative Bases for Jurisdiction

Jurisdiction over data, like other intangible assets is thus to be exercised to achieve the objectives listed above, using the twin parameters of state interest and fairness. India’s interests mean that the following ought to be putative bases for exercising jurisdiction in a data protection law:

- (i) All personal data of persons present in India that is processed must be protected. This can be ensured by exercising jurisdiction over personal data which is processed in India. If personal data is collected, disclosed, shared or

⁵⁴ Jennifer Daskal, The Un-territoriality of data, 125 Yale Law Journal (2015) at pp. 329-330.

⁵⁵ Andrew Keane Woods, Against Data Exceptionalism, 68 Stanford Law Review (2016) at p. 735.

⁵⁶ Andrew Keane Woods, Against Data Exceptionalism, 68 Stanford Law Review (2016) at p. 761.

⁵⁷ Jack Goldsmith, Unilateral Regulation of the Internet: A modest defence, 11(1) European Journal of International Law (2000) at p.136.

- otherwise processed in India, the law will apply to the processing of such personal data irrespective of the following facts: where the fiduciary is incorporated; where the processing or any subsequent processing takes place. This is based on the principle of territoriality⁵⁸ and passive personality.
- (ii) Personal data processed by Indian companies must be protected, irrespective of where it is actually processed. This is based on the principle of nationality as the company is located/incorporated within one's jurisdiction.
 - (iii) Personal data processed in India by foreign entities must be protected. Similar to the ground above, any processing in India is within the scope of Indian law on the basis of territoriality, irrespective of the nationality of the entity processing it.

While grounds (ii) and (iii) are straightforward, ground (i) is an exercise of long-arm jurisdiction.⁵⁹ This entails the state exercising extra-territorial jurisdiction on the ground that the actions elsewhere lead to significant effects in the state which require redressal. Such exercise, if resorted to by all states, might lead to a situation of considerable jurisdictional conflict. To prevent this, exercise of such jurisdiction must be carefully calibrated, keeping in mind the parameter of fairness. As a consequence, the following actions, despite being included on the basis of state interest, *ought to be excluded* from the application of the law:

- a. **Irregular and ad hoc collection of data of persons present in India:** Despite attempts by some countries and private entities making the internet a walled garden for its citizens and consumers, the internet is free to access and use from any jurisdiction. This is central to our conception of a free digital economy. Thus, any website operating out of any foreign jurisdiction which is accessed by a person present in India may collect and process some personal data relating to such person. They should not be disincentivised from doing so.

If such personal data is collected and further processed but is neither large-scale nor capable of causing significant harm in case of misuse, Indian law should not apply to this case. If this were to be done, every entity on the internet would have to comply with a plethora of laws on the basis of the off-chance that an individual from that country would access the service. To ensure the steady development of the internet as a freely accessible platform and treat data fiduciaries in other jurisdictions fairly, India should desist from making its law applicable to these instances. This would constitute an exception to putative bases (i), (ii) and (iii) discussed above. For example, a globally popular music streaming app is not available in India. However, some Indians may access it, either abroad or through usage of a virtual private

⁵⁸ Part of the cause of action in respect of transactions over the internet may occur in India even if there is no server in India involved. See *World Wrestling Entertainment, v. M/S Reshma Collection & Ors* 2014 SCC OnLine Del 2031

⁵⁹ *Banyan Tree Holding v. A.S. Murali Krishna* 2010(42)PTC 361; See *Mark Gergen, Constitutional Limitations on State Long Arm Jurisdiction*, 49(1) University of Chicago Law Review (1982).

network. This will not make the company subject to the Indian data protection law.

On the other hand, there may be cases of fiduciaries not physically present in the territory of India operating websites which must be regulated under Indian law. These include cases where such fiduciaries carry on business or systematically offer goods or service in India through the internet. This would go towards covering those entities that have a significant economic presence in India. Courts in India, while adapting conventional rules of jurisdiction to businesses carried on over the internet have distinguished between passive websites and others which target viewers in the forum state for commercial transactions resulting in harm in the forum state.⁶⁰ Recognising the nature of transactions over the internet, courts have interpreted the Trademarks Act and the Copyright Act to apply to persons not resident in India who nonetheless carry on business within the jurisdiction of the court.⁶¹

In addition to any link on the basis of systematic commercial activity, the law must also apply to activities such as profiling which pose considerable privacy harms which could be undertaken by fiduciaries that are not present within the territory of India. This would go towards covering those entities which have a significant digital presence for Indians though they may not have a significant economic presence. It is critical that such activities are regulated under Indian law.

An appropriate balance between these interests would be to restrict the application of the law in case of fiduciaries not present in India to those carrying on business in India or other activities such as profiling which could cause privacy harms to data principals in India.

b. Processing of data that is not personal data of persons present in India by an entity in India:

This is an exception to the principle of territoriality based on policy considerations of India having a large business process outsourcing industry handling large amounts of personal data of foreign nationals.⁶² While the

⁶⁰ Banyan Tree Holding v. Murali Krishna 2010 (42) PTC 361 “This Court holds that jurisdiction of the forum court does not get attracted merely on the basis of interactivity of the website which is accessible in the forum state. The degree of the interactivity apart, the nature of the activity permissible and whether it results in a commercial transaction has to be examined”. Further see Justice S. Muralidhar, Jurisdictional issues in Cyberspace, 6 The Indian Journal of Law and Technology (2010), “a lone trap transaction may not demonstrate the “purposeful” targeting by the defendant of the forum State or of “aiming” at particular customers therein. A more systematic behaviour over a series of transactions will have to be shown as having been entered into by the defendant.”

⁶¹ Icon Health and Fitness, Inc. v. Sheriff Usman and Ors. 2017 SCC OnLine 10481 relying upon World Wrestling Entertainment v. M/S Reshma Collection & Ors 2014 SCC OnLine Del 2031.

⁶² The IT-business process management sector revenues were estimated at around USD 130 billion in FY 2015-16 and USD 154 billion in FY 2016-17. The contribution of the IT sector to India’s GDP stood at 7.7% in 2016. It is estimated that the sector will expand at a compound annual growth rate of 9.5% to USD 300 billion by

general principle of jurisdiction would require compliance with Indian law, to facilitate smooth continuance of business, an exemption may be provided to such industries on the condition that no personal data of Indians are collected or further processed there. This would constitute an exception to putative bases (ii) discussed above.

On this basis, the proposed law should apply to:

1. Processing of personal data collected, used, shared, disclosed or otherwise processed in India (Territoriality).
2. To ensure that the jurisdiction under clause (1) is not overbroad, personal data collected of persons present in India, directly by fiduciaries not present in India who are not carrying on business in India or offering goods and services in a targeted and systematic manner to persons in India, or processing personal data in connection with profiling of data principals in India, may be excluded;
3. Personal data collected, used, shared, disclosed or otherwise processed by Indian companies, irrespective of where it is actually processed. However, the data protection law may empower the Central Government to exempt such processors which only process the personal data of foreign nationals not present in India (Territoriality).

II. Retrospective and Transitional Application of the Data Protection Law

The time at which the data protection law comes into effect will have to take into account the twin interests of effective enforcement and fairness to data fiduciaries. It is thus commonsensical that the law will not have retrospective application, i.e. it will not apply to any processing activity that has been completed prior to this law coming into effect.

However, it is essential to keep in mind that if there is any ongoing processing activity at the time the law comes into effect, then the data fiduciary must ensure that it is in compliance with this law in relation to that activity. The subject matter of application of a data protection law is the processing of personal data and not personal data itself. This means that merely because some personal data has been collected prior to the commencement of the law, such personal data is not excluded from the application of the law. In this context, the term ‘processing’ is a broad term understood to include any kind of operation on personal data, ranging from complex analysis and indexing to mere storage. As long as such processing is ongoing after the law coming into force, it will be covered. On the other hand, if the processing is complete before the law comes into force, the law will not be applicable to such processing. For example, if a bank has retained the personal data of an account holder, the law will be applicable to such storage as soon as it comes into force. However, if the bank has deleted the personal data before the law comes into force so as to close the account, the law will not be applicable.

2020. See IT & ITeS Industry in India, Indian Brand Equity Foundation, available at <<https://www.ibef.org/industry/information-technology-india.aspx>> (last accessed on 23 April 2018).

At the same time, it must be noted that the data protection law is the first of its kind in India and involves the creation of an entirely new regulatory framework for the purpose of its enforcement. Thus, in imposing several obligations on data fiduciaries, it is important to provide enough time to facilitate the seamless application of the law. Further, several obligations created by the law require significant organisational changes in data fiduciaries. Therefore, the Committee is of the view that the law should come into force in a structured and phased manner. Provisions relating to the establishment of the DPA and its functions should come into force first, followed by most substantive obligations on data fiduciaries. Certain obligations however, such as requirements for storage and processing of personal data within the territory of India, may require longer time. Provision for such staggered enforcement will be made.

RECOMMENDATIONS

- The law will have jurisdiction over the processing of personal data if such data has been used, shared, disclosed, collected or otherwise processed in India. However, in respect of processing by fiduciaries that are not present in India, the law shall apply to those carrying on business in India or other activities such as profiling which could cause privacy harms to data principals in India. Additionally, personal data collected, used, shared, disclosed or otherwise processed by companies incorporated under Indian law will be covered, irrespective of where it is actually processed in India. However, the data protection law may empower the Central Government to exempt such companies which only process the personal data of foreign nationals not present in India. **[Sections 2 and 104 of the Bill]**
- The law will not have retrospective application and it will come into force in a structured and phased manner. Processing that is ongoing after the coming into force of the law would be covered. Timelines should be set out for notifications of different parts of the law to facilitate compliance. **[Section 97 of the Bill]**

CHAPTER 3: PROCESSING

Complementing the territorial application of the law is the question of its subject matter application. The chapter on territorial application is premised on the general principle that personal data of Indians is to be protected in a manner that prevents harm and promotes a free and fair digital economy. Harm, much like benefits, is a possible consequence of processing of data, understood in its broadest sense to mean its collection, storage, use, disclosure and sharing. The scope of the legal framework must thus cover all processing of personal data. Further, certain categories of personal data may be likely to cause greater harm, or harm of a graver nature. Such data, widely termed ‘sensitive personal data’ and needs to be delineated specifically.

To prevent harm from the processing of personal data, whether sensitive or otherwise, requires regulation of processing activities. In our framework, one central component of such regulation is the consent of the data principal. There are two principled advantages of consent — first, it respects user autonomy; second, it provides a clear basis for the entity to whom consent is given to disclaim liability regarding matters to which such consent pertains. However, consent on the internet today may not be entirely effective in allowing individuals to understand what they are consenting to. The dissonance between what consent is and what it ought to be in order to be normatively meaningful, is vast.

This report outlines a modified notice and choice framework that incentivises meaningful, informed consent being asked for and given. This includes related and critical issues of a child’s consent and heightened safeguards for sensitive personal data processing. It is also imperative to recognise that the public good of the free and fair digital economy requires a consideration of collective benefits of data sharing, particularly in cases of legitimate state interest. Such consideration operates vis-à-vis both fiduciaries and principals.

In relation to data fiduciaries, there is an emerging need to recognise a new category of information as community data. This is information that is valuable owing to inputs from the community, which might require protection in addition to individuals’ personal data. The outline for such protection concludes this chapter.

In relation to principals, data may be processed on certain grounds other than consent, where legitimate state interests exist. These might take the form of exemption to the rule of seeking consent alone or a wider exemption from substantive obligations in the law. Chapter 8 will outline these areas of non-consensual grounds of processing.

A. White Paper and Public Comments

With regard to issues of scope and applicability, the provisional view of the White Paper was that since the object of the law was to protect informational privacy rights, the law should

only apply to natural persons, and should cover both private and public sector.⁶³ Commenters were in favour of applying the law to only natural persons since juristic persons enjoyed other protections such as intellectual property rights, contractual rights, etc. While some commenters favoured treating the public and private sector at par, those who did not, argued on the basis of them performing different functions.

Personal data was defined by the White Paper as any data from which an individual is identified or identifiable or reasonably identifiable, with the identifiability capable of being both direct and indirect.⁶⁴ Thus any data relating to an individual, including opinions or assessments, irrespective of accuracy should be accorded protection.⁶⁵ With regard to processing of personal data, the White Paper argued for a broad definition that could incorporate new operations by way of interpretation.⁶⁶ It was however felt that the three main types of processing viz. collection, use and disclosure should be mentioned and the law should cover both manual and automated processing.⁶⁷ Further, it was felt that data controllers and processors should be separately defined and that imposition of obligations on data processors be weighed against compliance costs.⁶⁸

Most commenters preferred the term ‘personal data’ with a broad definition to cover all types of data. One commenter pointed out that the law, like the law on intellectual property which was agnostic to quality, should be agnostic to accuracy and the law should specially cover opinions due to their ability to cause harm in the event of being inaccurate.⁶⁹ While commenters agreed that identification should be the standard for determining personal data, there was no consensus on what standard should be employed. Commenters preferred an inclusive definition of processing as opposed to an exclusive definition. There was also consensus on including both automated and manual modes of processing of personal data. With respect to defining entities such as ‘data controllers’ and ‘data processors’, there was significant divergence amongst commenters. Due to difficulties in defining such terms with

⁶³ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 32.

⁶⁴ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 39.

⁶⁵ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 39.

⁶⁶ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 46.

⁶⁷ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 46.

⁶⁸ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 51.

⁶⁹ Comments in response to the White Paper submitted by Sagnik Sarkar on 17 December 2017, available on file with the Committee.

precision, some commenters believed that all entities under the law should be carefully regulated.

Categories of data such as health information, genetic information, religious beliefs and affiliations, sexual orientation, racial and ethnic origin were considered as sensitive personal data by the White Paper.⁷⁰ The White Paper also recognised that processing of certain kinds of personal data due to the nature of the information had the likelihood of causing more harm to individuals and therefore required heightened levels of protection.⁷¹ The commenters, for the same reasons, were in favour of including a category of ‘sensitive personal data’. While there was no conclusive position with regard to what categories of personal data qualified as ‘sensitive personal data’, a significant number of commenters agreed with the suggestions in the White Paper. Some new categories were recommended including biometric data, passwords, trade union membership and Aadhaar number. Commenters suggested that there should be narrow grounds for processing of sensitive personal data. Additional safeguards for processing could take the form of technological and organisational safeguards.

The White Paper considered consent as a ground for the collection of personal data.⁷² However, it was recognised that in practice, since consent could be used to disclaim liability, therefore the validity and meaningfulness of consent be carefully determined.⁷³ It was felt that consent should be freely given, informed and specific to the processing of personal data.⁷⁴ Notice was also viewed as an important requirement, since it operationalised consent.⁷⁵ Measures such as codes of practice, data protection impact assessments, data trust scores and consent dashboards were suggested as means to better employ notice requirements.⁷⁶ A large number of commenters opted for consent being the primary ground of processing, whereas an equal number argued that it be treated at par with other grounds. One commenter, however, argued that consent was not the only way to empower individuals due

⁷⁰ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 43.

⁷¹ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 116.

⁷² White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 83.

⁷³ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 83.

⁷⁴ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 83.

⁷⁵ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 97.

⁷⁶ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed 20 April 2018) at pp. 97-98.

to the inapplicability of consent in some situations and presence of better alternatives.⁷⁷ In order to avoid consent fatigue, measures such as better notice design⁷⁸ and use of consent management architecture⁷⁹ were suggested.

The White Paper recognised children as a vulnerable group in need of a higher standard of protection.⁸⁰ Suggestions in this regard included parental authorisation for processing of personal data relating to children or only restricting such an authorisation for children of a very young age.⁸¹ Alternately, the White Paper suggested that distinct provisions be carved out which prohibit the processing of children's data for harmful purposes.⁸² A majority of commenters felt that the law should have special provisions to protect children's data, without being too paternalistic. Some did not comment on the issue, or were of the opinion that there was no need for special provisions since parental consent was sufficient to validate child's consent. Further, a majority of the commenters were unequivocal about there being no restrictions on prohibiting the processing of children's data or preventing them from accessing the internet due to free speech considerations.

B. Analysis

I. Building Blocks of the Law

(a) Personal Data

The breadth of protection that the law will offer depends on the definition of the term personal data. Since the 1980s, the standard for determining whether data is personal has been whether such data is related to an identified or identifiable individual.⁸³ Most jurisdictions studied by us employ some version of this formulation. The protection of any data that relates to an identifiable individual intuitively fits the objective of protecting an individual's identity.⁸⁴

⁷⁷ Comments in response to the White Paper submitted by the Center for Information Policy Leadership on 31 January 2018, available on file with the Committee.

⁷⁸ Comments in response to the White Paper submitted by AZB & Partners on 31 January 2018, available on file with the Committee.

⁷⁹ Comments in response to the White Paper submitted by Joseph Hungin on 31 January 2018, available on file with the Committee.

⁸⁰ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 89.

⁸¹ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 89.

⁸² White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 89.

⁸³ See OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013) available at <<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonald.htm>> (last accessed on 1 May 2018).

⁸⁴ Puttaswamy, (2017) 10 SCALE 1.

This standard of identifiability has served data protection very well over the years. However, developments in data science have considerably changed the understanding of identifiability.⁸⁵ Data no longer exists in binary states of identifiable or non-identifiable.⁸⁶ For instance, whether dynamic IP addresses constitute data about an identifiable individual depends on whether the person processing the data has additional data that enables the identification of the individual.⁸⁷ The degree of identifiability of an IP address may also be contextual in a different sense as several persons could be using the same machine. With advancements in technology, more and more identifiers of this nature are expected to emerge.⁸⁸

A related challenge to identifiability arises from the failure of methods of de-identification.⁸⁹ Various studies have indicated in some circumstances that it may be possible to identify individuals from data sets which are seemingly anonymised.⁹⁰ Anonymisation refers to the process of removing identifiers from personal data in a manner ensuring that the risk of identification is negligible.⁹¹ In some jurisdictions that were studied, such as the EU and South Africa, anonymised data falls outside the scope of data protection law.⁹² Jurisdictions like the EU have also explicitly endorsed pseudonymisation,⁹³ a method by which personal identifiers are replaced with pseudonyms.⁹⁴ The manner in which the law should address these methods is also linked to the question of identifiability.

These concerns, however, do not necessarily lead to the conclusion that the standard of identifiability must be abandoned. In fact, despite the criticism, there is no alternative which provides a workable standard for demarcating data that must be protected under the law. In these circumstances, a definition of personal data centred on identifiability must be constructed with the full awareness that its scope will, in many cases, depend on the context

⁸⁵ Ira Rubenstien, Identifiability: Policy and Practical Solutions for Anonymisation and Pseudonymisation available at <https://fpf.org/wp-content/uploads/2016/11/Rubinstein_framing-paper.pdf> (last accessed on 11 May 2018); OECD, OECD Digital Economy Papers No. 229, Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines available at <<https://www.oecd-ilibrary.org/docserver/5k3xz5zmj2mx-en.pdf?expires=1526295425&id=id&accname=guest&checksum=27E40D67E438BF316639AB9B943AD5F0>> (last accessed on 11 May 2018) at p. 10.

⁸⁶ OECD Digital Economy Papers No. 229, Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines available at <http://www.oecd-ilibrary.org/science-and-technology/privacyexpert-group-report-on-the-review-of-the-1980-oecd-privacy-guidelines_5k3xz5zmj2mx-en> (last accessed on 11 May 2018) at p. 10.

⁸⁷ Patrick Breyer v. Bundesrepublik Deutschland, Court of Justice of the EU, Case C-582/14 (judgment dated 19 October 2016).

⁸⁸ Paul Ohm, Broken Promises of Privacy: Responding to the surprising failure of Anonymisation, 57 UCLA Law Review (2010) at p. 1742.

⁸⁹ Paul Ohm, Broken Promises of Privacy: Responding to the surprising failure of Anonymisation, 57 UCLA Law Review (2010) at p. 1742.

⁹⁰ Paul Ohm, Broken Promises of Privacy: Responding to the surprising failure of Anonymisation, 57 UCLA Law Review (2010) at pp. 1717 to 1722.

⁹¹ Mark Elliot, Elaine Mackey, Kieron O'Hara and Caroline Tudor, The Anonymisation Decision-Making Framework (UKAN, 2016).

⁹² See Recital 26, EU GDPR; Section 6, POPI Act.

⁹³ Article 4 (5), Article 25 and Article 32, EU GDPR.

⁹⁴ Mark Elliot, Elaine Mackey, Kieron O'Hara and Caroline Tudor, The Anonymisation Decision-Making Framework (UKAN, 2016).

in which the relevant data is being processed. Bearing this mind, we believe that a broad and flexible definition of personal data should be adopted.

Identifiability in circumstances where the individual is directly identifiable from the presence of direct identifiers such as names⁹⁵ is perhaps uncontroversial and will obviously be included within the scope of any definition of personal data. The definition should also, in addition, apply to contexts where an individual may be indirectly identifiable from data that contains indirect identifiers.⁹⁶ Whether indirect identification is possible is often a question of the means available to a data fiduciary and the nature of data available to the fiduciary to combine with the original data. The question of means could also be related to cost and prevalence of methods of analysis having regard to the state of technology. Thus, even where an individual is not directly identifiable, data about such an individual must be treated as personal if it is possible that he or she may be identified having regard to these factors.

Thus, the definition of personal data will necessarily have to be in the form of a standard capable of applying to various contexts in which the data of a person may be processed. However, expressing a definition in the form of a standard without clearly demarcating the kinds of data that are protected may not be sufficient. Flexibility in the definition should not be achieved at the cost of certainty. Here, the role of the DPA will be critical. From time to time, the DPA will have to offer guidance, explaining the standards in the definition as applied to different categories of data in various contexts, especially with regard to newer categories of data developed as a result of advances in technology.

A slightly different approach may be adopted with respect to de-identification, pseudonymisation and anonymisation. It must be acknowledged that there is no consensus on the meanings of these terms and commenters have noted that policy makers and on occasion, legislators have been imprecise in their use of these terms.⁹⁷ Polonetsky *et al* bring about a measure of clarity to these terms by analysing a spectrum of identifiability that has data that is obviously personal on one end and anonymised data on the other.⁹⁸ Pseudonymised data and de-identified data are inflection points on the spectrum nearer to anonymisation.

Anonymisation requires the use of mathematical and technical methods to distort data to irreversibly ensure that identification is not possible.⁹⁹ In this aspect, anonymisation is distinct

⁹⁵ Polonetsky, Tene and Finch identify names, social security numbers and other basic contact information as direct identifiers in Polonetsky, Tene and Finch, *Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification*, 56 Santa Clara Law Review (2016) at p. 605. See also definition of identifiable individual in Article 4 (1) of the EU GDPR for a list of identifiers.

⁹⁶ Date of Birth, Age gender, Zip Code etc. have been suggested to be indirect identifiers in Polonetsky, Tene and Finch *Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification*, 56 Santa Clara Law Review (2016) at p. 605.

⁹⁷ Polonetsky, Tene and Finch, *Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification*, 56 Santa Clara Law Review (2016) at p. 596.

⁹⁸ Polonetsky, Tene and Finch, *Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification*, 56 Santa Clara Law Review (2016) at p. 609.

⁹⁹ Polonetsky, Tene and Finch, *Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification*, 56 Santa Clara Law Review (2016) at p. 618.

from de-identification which involves the masking or removal of identifiers from data sets to make identification more difficult.¹⁰⁰ Given the pace of technological advancement, it is desirable not to precisely define or prescribe standards which anonymisation must meet in the law. It is appropriate to leave it to the DPA to specify standards for anonymisation and data sets that meet these standards need not be governed by the law because they cease to be personal data.

A general standard in the definition of anonymisation regarding the possibility of identification, should be sufficient to guide the DPA in prescribing these standards. While the possibility of identification must be eliminated for a data set to be exempted from the rigours of the law, any absolute standard requiring the elimination of every risk including extremely remote risks of re-identification may be too high a barrier and may have the effect of minimal privacy gains at the cost of greater benefits from the use of such data sets.¹⁰¹

For other techniques of removing or masking identifiers from data including pseudonymisation, we adopt the term de-identification. The use of such techniques is encouraged and forms an important component of privacy by design. Despite the removal of identifiers from data, de-identified data carries with it a higher risk of re-identification.¹⁰² Hence it is appropriate to continue to treat de-identified data as personal data. Here again, the precise standards that these processes must meet will be specified by the DPA from time to time. In addition to technical standards, this could also include specification of measures for safekeeping of the key or additional information that could lead to re-identification from pseudonymised data.

(b) Sensitive Personal Data

Most data protection legislations set out the rules or grounds in accordance with which personal data may be processed to prevent any harm to data principals. However, it has been observed that despite the existence of such rules or grounds, the processing of certain types of data (usually relating to an integral part of an individual's identity)¹⁰³ could result in greater harm to the individual. Consequently, processing of these types of data will require stricter rules or grounds in law to minimise such harm.

While there has been no clear-cut approach towards categorising sensitive personal data, some authors have suggested a contextual approach, i.e., where any personal data can become sensitive depending on the circumstances and the manner in which it is being processed.¹⁰⁴

¹⁰⁰ Mark Elliot, Elaine Mackey, Kieron O'Hara and Caroline Tudor, The Anonymisation Decision-Making Framework (UKAN, 2016) at p.16.

¹⁰¹ Polonetsky, Tene and Finch, Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification, 56 Santa Clara Law Review (2016) at p. 619.

¹⁰² Mark Elliot, Elaine Mackey, Kieron O'Hara and Caroline Tudor, The Anonymisation Decision-Making Framework (UKAN, 2016) at p.16.

¹⁰³ Edward J. Bloustein, Privacy as an Aspect of Human Dignity- An Answer to Dean Prosser (New York University, School of Law, 1964).

¹⁰⁴ Helen Nissenbaum, Privacy as Contextual Integrity, 79(11) Washington Law Review (2004).

However, this approach may place significant burden on data fiduciaries and regulatory resources as they would have to determine whether the personal data in question is sensitive or not, and whether it is capable of causing great harm to the individual, on a case by case basis. Therefore, by identifying certain types of data as sensitive in the law itself, and setting out specific obligations that must be met by the data fiduciary while processing such data, potentially significant harms may be pre-empted.

Data sensitivity, in one view, can depend on the legal and sociological context of a country.¹⁰⁵ However, certain categories of personal data are capable of giving rise to privacy harms regardless of context and an objective method of identifying such kinds of data becomes necessary. Hence, we have considered the following criteria to categorise what is ‘sensitive’:

- (i) the likelihood that processing of a category of personal data would cause significant harm to the data principal;
- (ii) any expectation of confidentiality that might be applicable to that category of personal data;
- (iii) whether a significantly discernible class of data principals could suffer harm of a similar or relatable nature;¹⁰⁶
- (iv) the adequacy of general rules to personal data.

Based on the above criteria, the Committee has thought fit to categorise the following as sensitive personal data under a data protection law:

- a. Passwords;
- b. Financial data;
- c. Health data;
- d. Official identifiers which would include government issued identity cards;
- e. Sex life and sexual orientation;
- f. Biometric and genetic data;
- g. Transgender status or intersex status;¹⁰⁷
- h. Caste or tribe; and
- i. Religious or political beliefs or affiliations.

¹⁰⁵ See Karen McCullagh, Data Sensitivity: Proposals for Resolving the Conundrum, 2(4) Journal of International Commercial Law and Technology (2007) at p. 191.

¹⁰⁶ Please note that these factors are adapted from those identified by Paul Ohm in Sensitive Information, 88 Southern California Law Review (2015) at p. 35.

¹⁰⁷ Personal data revealing the condition of a person as being transgender or intersex should be protected as sensitive personal data. The additional protection afforded by this categorisation is required due to the discrimination that they may be subjected to in society. Such persons are free to reveal their status voluntarily. We understand a transgender person to be one whose gender does not match the gender assigned to them at birth. On the other hand, an intersex person is one who is neither wholly female nor wholly male, or a combination of female or male, or neither female nor male (this may be due to physical, hormonal or genetic features).

However, a residuary power will be vested with the DPA to list out further categories of sensitive personal data on the basis of the above criteria. This power has been considered necessary due to the impracticability of laying down an exhaustive enumeration at the time of drafting. Harm can be caused by the processing of sensitive personal data *per se* or if it is aggregated for profiling. Consequently, the DPA will be granted a residuary power to list categories of sensitive personal data on the basis of both these sources of harm, as and when it considers necessary. Thus, for instance, geo-location data may be considered for listing as a category of sensitive personal data in the future since it may lead to harm upon aggregation.

II. Consent

The notice and choice framework to secure an individual's consent is the bulwark on which data processing practices in the digital economy are founded. It is based on the philosophically significant act of an individual providing consent for certain actions pertaining to her data.¹⁰⁸ Consent has been viewed as an expression of a person's autonomy or control, which has the consequence of allowing another person to legally disclaim liability for acts which have been consented to.¹⁰⁹ This is enabled through notice — an affirmative obligation placed upon data fiduciaries to communicate the terms of consent.¹¹⁰ It should be understood that while notice as an obligation plays an important role alongside consent, it is also a crucial obligation even where processing takes place on the basis of grounds other than consent. Further nuances on the application of this obligation may be found in Chapter 4 and in Chapter 8 where the application to one of these grounds has been discussed.

A preponderance of evidence points to the fact that the operation of notice and consent on the internet today is broken.¹¹¹ Consent forms are complex and often boilerplate. Consequently, individuals do not read them; even if they attempt to, they might not understand them; even if they understand them, provisions to give meaningful consent in a granular fashion are absent.¹¹² Any enumeration of a consent framework must be based on this salient realisation: on the internet today, consent does not work.

¹⁰⁸ Ryan M. Calo, Against Notice Skepticism in Privacy (and Elsewhere), 87(3) Notre Dame Law Review (2012) at p. 1049; Per Sanjay Kishan Kaul, J., in *Puttaswamy*, (2017) 10 SCALE 1 at p. 30 referring to the Second Circuit's decision in *Haelan Laboratories v. Topps Chewing Gum*. 202 F.2d 866 (2d Cir. 1953) penned by Judge Jerome Frank.

¹⁰⁹ Adam Moore, Toward Informational Privacy Rights, 44 San Diego Law Review (2007) at p. 812; Anita L. Allen, Why privacy isn't everything: Feminist reflections on personal accountability (Rowman & Littlefield, 2003) at pp. 115-16; John Kleinig, The Nature of Consent in The Ethics of Consent- Theory and Practice (Alan Wertheimer and Franklin Miller (eds.), Oxford University Press, 2009) at p. 4.

¹¹⁰ Ryan M. Calo, Against Notice Skepticism in Privacy (and Elsewhere), 87(3) Notre Dame Law Review (2012) at p. 1031.

¹¹¹ Ryan M. Calo, Against Notice Skepticism in Privacy (and Elsewhere), 87(3) Notre Dame Law Review (2012) at p.1031; Reidenberg et al, Privacy Harms and the Effectiveness of the Notice and Choice Framework, 11(2) Journal of Law and Policy for the Information Society (2015); Florian Schaub et al, A design space for effective Privacy Notices (Symposium on usable privacy and security, 2015) at p. 2; LF Cranor, Necessary but not sufficient: Standardized mechanisms for privacy notice and choice, 10 Journal on Telecommunications and High Technology Law (2012) at p. 273.

¹¹² See B. W. Schermer et al, The crisis of consent: how stronger legal protection may lead to weaker consent in data protection, 16(2) Ethics and Information Technology (2014).

Despite these lacunae, individuals regularly consent to data collection and use practices as per the privacy policy or terms and conditions of the websites visited, applications downloaded, or programmes signed in to. So prevalent have such boilerplate contracts become in the online world, that courts too have often recognised their legal validity, irrespective of the unequal bargaining power of parties and doubts about how informed the giving of consent might have been.¹¹³

This has led to calls to do away with the individual's consent as a ground for processing completely¹¹⁴ including in responses to the White Paper.¹¹⁵ This conclusion is hasty. The problems with consent highlighted above relate to the efficacy of consent as a method of protecting personal data and consequently preventing individual harm. These are practical concerns rather than normative ones relating to the value of autonomy in a data protection framework. It would be inappropriate to dispense with the normative value of consent itself owing to the way in which it operates in practice currently. Rather, a modified framework for operationalising consent needs to be found.

(a) A revised operational framework for consent

If consent is still seen as a normatively significant expression of autonomy, the critical missing element in its operation is a revised operational framework for making such expression effective. The philosophical underpinnings of such a framework are provided by Arthur Leff in his seminal article 'Contract As Thing'.¹¹⁶

Leff contends that consumer contracts (of which online contracts are a manifestation) share no significant similarities with contracts *per se*- only one party sets the terms, with no opportunity for the other party to negotiate such terms; further, there is no 'bargain, agreement, dicker, process, mutability, becoming'¹¹⁷ which are standard features of contracts. These 'contracts of adhesion' are not based on informed consent or mutual common understanding.¹¹⁸

He proposes instead to treat such contracts as 'things' *per se*, i.e., products. This would be in keeping with the limitations of contract law, which regulates the process of contracting,

¹¹³ See for example, TradeComet.com LLC v. Google, Inc., 693 F. Supp. 2d 370, 377 (S.D.N.Y. 2010); Fteja v. Facebook, Inc., 841 F.Supp.2d 829 (S.D.N.Y. 2012).

¹¹⁴ Daniel J Solove, Introduction: Privacy Self-Management and the consent dilemma, 126 Harvard Law Review (2013) at p. 1880; Rahul Matthan, Beyond Consent: A New Paradigm for Data Protection- Discussion Document 2017-03, Takshashila Institution, (2017) available at <<http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf>> (last accessed on 23 March 2018).

¹¹⁵ For instance, it was suggested that an accountability model should be adopted instead of consent being the primary ground of processing, see Comments in response to the White Paper submitted by the Takshashila Institution on 30 January 2018, available on file with the Committee.

¹¹⁶ Arthur A. Leff, Contract As Thing, 19(2) American University Law Review (1970) at p. 131.

¹¹⁷ Arthur A. Leff, Contract As Thing, 19(2) American University Law Review (1970) at p. 147.

¹¹⁸ Andrew Robertson, The limits of voluntariness in contract, 29(1) Melbourne University Law Review (2005) at p. 179.

rather than the product at the end of it. Since a consumer contract is essentially a piece of paper over which there is no bargaining or agreement but merely evidence of the same, it is akin to a product which is exchanged at the end of the contracting process. Seeing an online contract in this manner allows us a wider operating arsenal to regulate notice and choice, i.e., the regime of product liability.¹¹⁹

(b) Consequences of such a Framework

The consequence of incorporating product liability into consent forms means that data fiduciaries will be liable, *as if* the consent form were a product.¹²⁰ This implies liability for any harm that is caused to a data principal pursuant to the latter providing consent, as a consequence of such processing.¹²¹ Harms can ensue either from the data fiduciary not adhering to the terms of the notice or the notice itself being in a form which is not compliant with the data protection law.

The key illustrative harms that we have identified are:

- (i) Such personal data is collected which are not those reasonably expected by the data principal;
- (ii) Purposes for which personal data sought are not those reasonably expected by the data principal;
- (iii) Disclosure and sharing of personal data is allowed with such persons and in such manner not reasonably expected by the data principal.

These would be analogous to traditional manufacturing defects in a product liability regime.¹²² Further:

- (i) Notice did not appear before application is installed;
- (ii) Pre-checked boxes existed;
- (iii) Appropriate standard of clarity of notice not met.

These would be analogous to traditional design defects in a product liability regime. Further:

¹¹⁹ See David G. Owen, *Products Liability Law* (Thomson West, 2008); further, the Central Motor Vehicle Rules, 1989 that mandate compliance with minimum safety standards regarding automobile components are an illustration of the application of product liability in India. A key distinction however may relate to the possibility of withdrawal of consent in the case of data processing which may not be applicable in Leff's framework.

¹²⁰ The usefulness of the construct of "as if" as a technique of analysis by noted philosopher Kwame Anthony Appiah. See Kwame Anthony Appiah, *As If: Idealisation and Ideals* (Harvard University Press, 2017). For the benefits and pitfalls of such analysis, see Thomas Nagel, "As If", *The New York Review of Books* (2018) available at <<http://www.nybooks.com/articles/2018/04/05/as-if-kwame-anthony-appiah/>> (last accessed on 10 May 2018).

¹²¹ *Greenman v. Yuba Power Products, Inc* (1963) 59 Cal.2d 57 [13 A.L.R.3d 1049]. The Supreme Court of California held that any entity involved in the chain of distribution for a defective product may be held liable for injuries caused by the defect.

¹²² *Wheels World v. Pradeep Kumar Khurana*, I (2008) CPJ 324 NC; *Tata Motors v. Rajesh Tyagi and HIM Motors Show Room*, 2014(1) C.P.C.267.

- (i) Potentially harmful/ burdensome/ onerous clauses of the contract were not pointed out specifically to the data principal.

This would be analogous to a marketing defect in a product liability regime.

Thus the substantive obligations on data fiduciaries in relation to the notice provided to data principals would *inter alia* be to:

1. Collect personal data necessary for providing service to the data principal to fulfil the purposes specified and disclose such data only to such persons as reasonably expected by the data principal.¹²³
2. Communicate (1) above through a clear notice.
3. Ensure that contractual terms that are potentially onerous or harmful do not escape the attention of the data principal.¹²⁴
4. Show notice before any such practices communicated in the notice take place.
5. Require affirmative consent from the data principal without any pre-checked boxes.
6. Provide requisite granularity thereby allowing data principals to access services without necessarily consenting to all or nothing.

(c) Enforcement of the Revised Framework

Enforcement tools relating to notice and consent will consist of the following:

- (i) Model forms may be laid down by the DPA through codes of practice. Adhering to such pre-approved forms will demonstrate compliance with notice and consent related provisions in the law and no liability regarding these limited obligations will apply.¹²⁵ Needless to say, this will not affect substantive liability, if any, for other obligations under the law or contract. Some of the methods in which a notice can be improved have been illustrated in the guidance document for effective notice which is annexed as **Annexure B**.¹²⁶
- (ii) If a non-model form, not meeting the prescribed standards, is used then any liability for non-compliance with legal requirements shall be enforced on the pain of penalty.

¹²³ This is discussed in further detail in Chapter 4 of this report.

¹²⁴ Lord Denning's use of the red hand for potentially unreasonable clauses in a contract may be instructive here. A manicule may also be used. See *J Spurling Ltd. v. Bradshaw*, [1956] 1 WLR 461.

¹²⁵ This is similar to model Articles of Association in the Companies Act, 2013. Section 5 read with Schedule I, Table F of the Companies Act, 2013. Section 5(6): The articles of a company shall be in respective forms specified in Tables F, G, H, I and J in Schedule I as may be applicable to such company; Section 5(7), Companies Act, 2013 provides that a company may adopt all or any of the regulations contained in the model articles applicable to such company.

¹²⁶ The Committee would like to thank an independent graphic designer, Ananya Khaitan for designing this model notice.

- (iii) Further, a data trust score (similar to a credit score) may be given to all significant data fiduciaries (a categorisation which has been outlined in Chapter 9), audited by data auditors and displayed prominently in the notice.
- (iv) Dynamic consent renewal (opt-in, requiring fresh consent or opt-out requiring simple notification with option to opt-out) will be provided for, depending on the type of data in question. A consent dashboard may be created for this purpose.¹²⁷ The relevant provisions may be developed through delegated legislation by the DPA as and when it considers necessary.

(d) Standard of Consent

The revised notice and choice framework is a design modification which makes data fiduciaries communicate the terms of consent to data principals in a clear form with substantive obligations delineated. In our view, this is a significant step towards ensuring that consent is informed and meaningful.

A question however might arise regarding the standard of clarity that might be required in communicating consent. The EU GDPR mandates that the consent must be freely given, specific, informed and unambiguous for processing of personal data. Consent has to be expressed by a “statement or by clear affirmative action”.¹²⁸ Certain jurisdictions are even more prescriptive, requiring particular font sizes, spacing, and more form-based conditions.¹²⁹

While it is the Committee’s view that the revised notice and choice framework as implemented through model forms prescribed by the DPA *per se* will provide sufficient clarity, the law will provide the conditions for validity of consent, requiring it to be ‘free’, ‘informed’, ‘clear’, ‘specific’ and ‘capable of being withdrawn’. These conditions are discussed in greater detail below.

There are two standards of consent envisaged under the proposed data protection bill, regular or ordinary consent, and explicit consent.

The ordinary standard of consent as envisaged under the draft Bill needs to meet five conditions mentioned above. Firstly, it must be *free*. This is to be determined having regard to section 14 of the Indian Contract Act, 1872. Consent is said to be free when it is not caused by coercion, undue influence, fraud, misrepresentation or mistake, and meets any other conditions as per contract law jurisprudence.

Consent needs to be *informed*, having regard to whether it communicates relevant information in compliance with the draft Bill’s provision on privacy notices.

¹²⁷ See Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016 for an instance of dashboard-based approach to consent in India.

¹²⁸ Article 4(11), EU GDPR.

¹²⁹ See Final Model Privacy Form under GLB Act (US) available at <https://www.ftc.gov/sites/default/files/documents/federal_register_notices/final-model-privacy-form-under-gramm-leach-bliley-act-16-cfr-part-313/091201gramm-leach.pdf> (last accessed on 26 April 2018).

Additionally, the consent needs to be *specific*, having regard to whether the data principal can choose to not consent to certain purposes of processing of their personal data. If a particular type of personal data is not necessary for the performance of a contract, the enjoyment of a legal right, or the provision of a good or service, then such performance, enjoyment or provision cannot be made conditional to the giving of consent by the data principal. This makes the consent specific, in that it is unbundled from contracts and rights.

Consent also must be *clear*, having regard to whether it communicates agreement to the relevant processing through an affirmative action that is meaningful in a given context. Thus, silence and pre-ticked checkboxes would be unlawful modes of obtaining consent. However, that does not mean that in some instances that consent cannot be implied. For example, when an association's membership form requests for details such as name, address, telephone number, professional designation, and marital status, the affirmative action of entering such details can amount to a clear expression of consent. This would depend on the context in which the form has been collected, including whether the form explains the purposes of processing this data. Here, no explicit written expression of their agreement to such processing activity needs to be given separately.

Lastly, consent needs to be *capable of being withdrawn* as easily as it was given.

(e) Different Standards for Different Types of Personal Data Processing

The standard described immediately above must not be understood to be a one size fits all model for giving consent. While the ordinary standard must be applicable in the processing of personal data generally, there is a need to clarify where it may be permissible for consent to be implied. Large amounts of personal data may be collected and processed on a regular basis to maintain databases and for other instances of routine processing. In a limited set of such instances, implied consent may be sufficient while in others it may not be adequate. Where consent may be implied, it should nevertheless be free, informed, clear and specific having regard to the circumstances. Fixing these standards in the law does not rule out the use of implied consent in contexts where it is appropriate.

On the other hand, for processing of sensitive personal data, an even higher standard of consent than the ordinary one described above must apply. In some jurisdictions this has taken the form of requiring 'explicit consent' in the law.¹³⁰ This is a useful formulation.

Of the five conditions of valid ordinary consent described above, three are enhanced for the purpose of explicit consent. This makes the term a heightened form of ordinary consent, rather than merely the opposite of implied consent. The standard of explicit consent goes beyond the mode of communication of the agreement. This is described below.

¹³⁰ Examples of such jurisdictions include EU (Articles 9(1) and 9(2)(a)-(j), EU GDPR), Canada (Schedule 1, Section 4.3.4 and Section 4.3.6, Principle 3- Consent, PIPEDA), US FTC's Behavioural Advertising Principles in the United States, FTC Staff Report: Self-Regulatory Principles for Online Behavioural Advertising (2009) available at <<https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf>> (last accessed on 27 April 2018).

Thus, to be *informed*, explicit consent should not just be in compliance with the provisions on notice under the draft Bill but must additionally draw the attention of the data principal to the purposes of, or operations in, processing activities that may result in significant consequences for her. While ordinary consent need only allow the data principal to choose between different purposes to be *specific*, explicit consent must additionally permit the choice between operations in, and different categories of, sensitive personal data relevant to processing. Finally, for explicit consent to be adequately *clear*, the expression of the consent should convey agreement to the processing objectively and without recourse to inference from conduct in a context. This would mean that if such an expression would not be meaningful in a different context, then it would not be adequate.

In the above example of an association's membership form, if the form also requires the collection of bank account details, then the mere act of entering data into the form cannot serve the purpose of expressing explicit consent. In order to meet the requisite standard of clarity, the data principal must not just enter the data, but must separately express that they consent to the relevant processing. A simple illustration of how this could be done is for her to write out her agreement to such processing. Other ways in which explicit consent can be expressed are by using a one time password (OTP). However, for this to be a sufficiently clear expression, the OTP provided to the data principal must be accompanied by a clear indication of what processing activity it would be authorising. Similarly, ticking a check-box which merely says 'I agree' would most likely not be considered explicit consent. However, it may be considered explicit if the check-box says 'I agree to the processing of the personal data entered above for the purpose of maintaining X Association's register of members, for communication of matters necessary for my membership in X Association and for transactions between the Association and myself.'

It is important to keep in mind that a large amount of personal data can be processed pursuant to the initial consent given by the data principal at the time of collection by the data fiduciary or any other party. Such consent will have to be as per the new framework and will be provided by the data principal for such processing as may be necessary to achieve the purposes for which consent is sought. The time for which such consent is valid is thus necessarily contingent on the purposes for which processing of personal data is sought. Where there are changes in such purposes or other relevant circumstances, the giving of such a sweeping consent would no more be adequate. In our view, the most efficacious mechanism for implementing ongoing consents is a consent dashboard.

(f) Consent Dashboard and Avoiding Consent Fatigue

A consent dashboard would enable data principals to keep track of consent for processing in real time and allow them to operationalise the right accorded to them under the data protection law. With the EU GDPR posing stringent requirements on data controllers to operationalise rights available to data subjects, various models for possible consent architectures that seek to enhance transparency have come up. For instance, Raschke *et al* envision two approaches. First, each fiduciary is required to operate its own dashboard; alternately, data principals have access to one dashboard operated by a third entity to manage

all fiduciaries they deal with.¹³¹ A fiduciary-operated model is easier to enforce since the whole process of transfers can be logged and recorded internally. A single point dashboard while being more convenient from the perspective of data principals would require significant interoperability.¹³²

A single point dashboard is akin to the one approved by the RBI in its Non-Banking Financial Company - Account Aggregator Directions.¹³³ The dashboard collects 'consent artefacts' of users, does not own any information but only provides information to the user in a consolidated manner. An aggregator that tracks consent, would thus only store the fact of the various consents given by the data principal to the different data fiduciaries and not ordinarily store any of the actual data.

We believe that comprehensive dashboards have significant potential in operationalising consent effectively. The opacity of consent and data sharing on the internet today is the foundation of several fears of data protection. Dashboards, if well implemented, can overcome this fear. However, if not carefully conceptualised and not made adequately simple, dashboards could become expensive white elephants.

Thus, for ease of enforcement, consent dashboards may be introduced in India in an incremental manner. The first approach where the fiduciary controls its own dashboard could be an initial step, while a central dashboard that coordinates with various fiduciaries can be introduced either sector-wise or universally over a period of time. This framework is recommendatory in nature and has been suggested to aid the resolution of the inherent problems of consent fatigue.

As a general comment, in much of the literature on notice and consent, critics of more robust protections use 'consent fatigue' almost like a slogan that brooks no disagreement. There is undoubtedly some truth in excessive consent requirements desensitising individuals towards consent. However this prospect only becomes real if it is envisaged that the principal will be continuously required to take affirmative action to demonstrate consent.¹³⁴ This is not an accurate factual premise in our framework. If data processing is in order to fulfil the purpose for which consent has been provided in accordance with law, one need not approach the individual for fresh consent. A notification may be sent to her via the dashboard of any processing necessary for fulfilment of such purpose. However, if personal data is used for other purposes, then fresh consent must be sought. If user fatigue ensues, then it is expected

¹³¹ P. Raschke et al, Designing a GDPR-compliant and Usable Privacy Dashboard, Technical University Berlin, Germany (2017) available at <<https://www.specialprivacy.eu/images/documents/IFIP-2017-Raschke.pdf>> (last accessed on 26 April 2018).

¹³² P. Raschke et al, Designing a GDPR-compliant and Usable Privacy Dashboard, Technical University Berlin, Germany (2017) available at <<https://www.specialprivacy.eu/images/documents/IFIP-2017-Raschke.pdf>> (last accessed on 26 April 2018).

¹³³ Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016.

¹³⁴ For instances of such criticisms, see B. W. Schermer et al, The crisis of consent: how stronger legal protection may lead to weaker consent in data protection, 16(2) Ethics and Information Technology (2014).

that data fiduciaries will, as responsible entities, not exacerbate such fatigue, and only use consent for purposes for which personal data is sought.¹³⁵

This does not entirely obviate concerns of fatigue. While browsing websites, constant intimations for consent may affect user experience and desensitise individuals to privacy harms.¹³⁶ To be sure, processing of personal data may take place while browsing a website. In the offline world, this is akin to being under surveillance when walking into a shopping mall. For such regularly occurring situations, just as in the offline world, no explicit consent is usually taken, and the DPA may have to specify alternate standards of consent. At all points of time, such determination must be based on the *ex ante* assessment of potential of harm from such processing.

(g) Consent and Contractual Necessity

Data protection laws in some jurisdictions create a separate ground for processing personal data where it is necessary for the performance of a contract.¹³⁷ Recourse to such a ground would permit processing in relation to a contract entered into by the data principal, including contracts for the provision of goods and services. For instance, if an individual purchases a television set on an e-commerce website, the site would be justified in processing her personal data (name, address and credit card details) under contractual necessity to deliver the product. For the processing activity to be necessary for the performance of the contract there would have to be a direct nexus between the processing of the data and the execution of the contract.¹³⁸ In other words, the data fiduciary would have to justify that without processing of the personal data, the obligations under the contract cannot be performed.

As seen in such laws, the ground of contractual necessity is de-coupled or unbundled from consent in that a person cannot be later forced into consenting to processing of that personal data which is not needed by the other party in performing its obligations under a concluded contract.¹³⁹ If consent to processing is extracted by holding contractual rights hostage in this manner, such consent cannot be treated as free.¹⁴⁰

¹³⁵ In user studies based on the existing legal framework in California, US, users showed little fatigue and preferred short, easy-to-understand, just-in-time notices, see A. McDonald & T. Lowenthal, Nano-Notice: Privacy Disclosure at a Mobile Scale, 3 Journal of Information Policy (2013).

¹³⁶ In an interesting study it was estimated that the national opportunity cost of reading privacy policies in the context of US was USD 781 billion, see A. McDonald and L. F. Cranor, The Cost of Reading Privacy Policies, 4(3) I/S: A Journal of Law and Policy for the Information Society (2008) at p. 544.

¹³⁷ See, for example, Article 6(1)(b), EU GDPR; Section 11(1)(b), POPI Act.

¹³⁸ Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679 (2018) at p. 8.

¹³⁹ The EU GDPR attempts to distinguish between consent and contract by ensuring that “the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract”. Article 7(4), EU GDPR provides: “When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.” See also Recital 43, EU GDPR and Article 29 Working Party Opinion, Guidelines on Consent under Regulation 2016/679 (2018) at p. 8.

¹⁴⁰ Recital 43, EU GDPR.

Some laws, such as Canada’s PIPEDA, do not set out such a ground.¹⁴¹ This means that entities have to largely rely on consent for processing instead of any ground on contract. Since a person consents to a contract, it may appear intuitive that such consent is also the justification for the processing of personal data that is necessary for the performance of the contract.

On the other hand, it may be noted that once a contract has been entered into, a party may not prevent its execution without facing legal consequences. Once a data principal contracts to receive delivery of a good, it is implied that the other party would require personal data such as the delivery address so as to make the delivery. It may not appear meaningful to subsequently make the processing of such data contingent on the consent of the data principal. Enforceable contracts also allow parties to plan their own actions while relying on the certainty of each other’s actions so as to secure the costs they incur. However, it is arguable that consent has to be capable of being withdrawn to be meaningful.¹⁴² Such withdrawals, in the context of a contract, would prevent the other party from performing its obligations. Ordinarily, contracts do not permit unilateral withdrawals.

The Committee has noted these distinctions between consent and contract. However, there is considerable concern that a ground relying on contractual necessity could be easily misused. For one, a data fiduciary may insert clauses regarding various unrelated data processing activities within a contract and justify processing by claiming that it is necessary for the performance of those clauses. For another, it is unclear whether processing is subject to any meaningful check when the processing of personal data is the very subject matter of the contract or in digital contexts that have a pervasive connection with the personal data of a data principal. These contracts may be in a standard form, often entered into without any opportunity for negotiation.

Were a ground of contractual necessity to exist, there is a risk that data fiduciaries would be free to process any personal data if the processing is necessary to perform the obligations that the fiduciary may have inserted into the contract unilaterally. Where the essential objectives of a contract are not clearly defined, it may not be clear what personal data is and is not necessary for its performance. This could result in the treatment of such data as the “price” for a transaction. There continues to be some debate as to whether it is appropriate to permit the use of personal data as “counter-performance”.¹⁴³

¹⁴¹ Clause 4.3, Schedule 1 and Sections 6.1 and 7 (1), (2), (3), (4) and (5), Part 1, Division 1, PIPEDA

¹⁴² Recital 42, EU GDPR (“Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.”)

¹⁴³ See, of instance, Article 3 of the Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, 2015/0287 (COD) available at <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015PC0634&from=EN>> (last accessed 9 July 2018) (referring to “counter-performance other than money in the form of personal data or any other data.”) Raising concerns regarding this formulation, the European Data Protection Supervisor has warned against “any new provision introducing the idea that people can pay with their data the same way as they do with money.” See European Data Protection Supervisor, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content (2017) available at

The Committee has attempted to mitigate these potential risks by opting to treat consent as the ground on which personal data is processed even where such data is necessary for the performance of a contract. However, where processing of personal data is necessary for a contract, the withdrawal of consent to such processing cannot be without consequences. If performance of the contract is sought to be refused, any legal consequences resulting from actions already taken by the other party in pursuance of the contract would have to be borne by the party preventing or refusing such performance.¹⁴⁴

While we are aware that this does not entirely solve the problems outlined above, we consider this approach advantageous for two reasons. First, where a data principal consents to a contract that requires personal data processing, such consent would have to meet the heightened standard under data protection law instead of the lower standard of contract law. Second, even though contracts may not ordinarily envisage unilateral withdrawal, such withdrawals will be permitted in the context of personal data. The data principal will have the freedom to select which specific parts of their consent they would like to withdraw. As consent has to be “specific” to be valid, it would now also be possible to withdraw it specifically from a contract. Insofar as such a withdrawal would prevent the performance of a specific clause in a contract, the data principal would be able to choose to face the specific consequences that flow therefrom and choose what parts of the contract they would like the other party to continue performing. The data principal cannot be compelled through private law remedies to part with their personal data or go along with processing of personal data that has already been collected. This would be subject to the severability of such clauses from the rest of the contract and where this is not possible, the other party would be justified in seeking whatever damages may flow from the breach of the contract.

III. Protection of Children’s Personal Data

It is widely accepted that processing of personal data of children ought to be subject to greater protection than regular processing of data.¹⁴⁵ The justification for such differential treatment arises from the recognition that children are unable to fully understand the consequences of their actions.¹⁴⁶ This is only exacerbated in the digital world where data collection and processing is largely opaque and mired in complex consent forms.

<https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf> (last accessed on 9 July 2018).

¹⁴⁴ See sections 39 (Effect of refusal of party to perform promise wholly) and 53 (Liability of party preventing event on which the contract is to take effect) of the Indian Contract Act, 1872.

¹⁴⁵ For instance, see COPPA, Article 8, EU GDPR., Sections 34 and 35 of the POPI Act.

¹⁴⁶ Sheri Bauman and Tanisha Tatum, Web Sites for Young Children: Gateway to Online Social Networking?, 13(1) Professional School Counselling (2009); Michelle Sargent, Misplaced Misrepresentations: Why Misrepresentation-of-Age Statutes Must be Reinterpreted as They Apply to Children’s Online Contracts, 112(2) Michigan Law Review (2013); Dale Kunkel, The Role of Research in the Regulation of U.S. Children’s Television Advertising, 12(1) Science Communication (1990) at pp. 101-119.

Safeguarding the best interests of the child should be the guiding principle for statutory regulation on protecting data of children. This is enunciated in the CRC, to which India is a signatory.¹⁴⁷ The implementation of this principle in the data protection law should operate in two ways. First, it shall be a freestanding legal obligation on *all* data fiduciaries, i.e., principles will develop on how all data fiduciaries must process data relating to children in their best interests. Second, it should take the following specific form in relation to identified categories of data fiduciaries:

(a) Identification of guardian data fiduciaries

At present, the Committee understands that there are two categories of data fiduciaries who may be processing personal data of children: first, services offered primarily to children (e.g. YouTube Kids app, Hot Wheels, Walt Disney);¹⁴⁸ second, social media services (e.g. Facebook, Instagram).¹⁴⁹ The DPA shall have the power to notify data fiduciaries who operate commercial websites or online services directed at children, or who process large volumes of personal data of children as ‘guardian data fiduciaries’.

(b) Who is a child?

In US, COPPA allows children 13 years of age and above to consent, whereas Article 8 of the EU GDPR mandates age 16 as the threshold, though allowing leeway for states to reduce the age of consent to 13. At the same time, the CRC defines a child as below 18 years of age under Article 1. This is also the age for anyone to validly enter into a contract in India as per Section 11, Contract Act.¹⁵⁰ The principled considerations for determining an age for consent are clear — protecting the child from harm while ensuring that she can autonomously participate in her own development.¹⁵¹

In order to determine the cut-off age, the choice should be governed by a balance of the following factors:

- (i) Principled considerations;
- (ii) The maximum age of 18 and the minimum age of 13 (considered as the relevant range in most literature and comparative jurisdictions);

¹⁴⁷ Article 3, CRC.

¹⁴⁸ Anthony Miyazaki et al, Self-Regulatory Safeguards and the Online Privacy of Preteen Children: Implications for the Advertising Industry, 38(4) Journal of Advertising (2009); Catherine Montgomery & Jeff Chester, Data Protection for Youth in the Digital Age: Developing a Rights-based Global Framework, 4 EDPL (2015).

¹⁴⁹ Sheri Bauman and Tanisha Tatum, Web Sites for Young Children: Gateway to Online Social Networking?, 13(1) Professional School Counselling (2009).

¹⁵⁰ Section 3, The Indian Majority Act, 1875 sets 18 as the age of majority. Under Section 11, Contract Act, persons who have attained the age of majority are competent to contract. In Mohori Bibee v. Dharmadas Ghose (1903) 30 Cal. 539 it was held that contracts entered into by minors are void ab initio. This position continues to remain valid today.

¹⁵¹ Simone van der Hof, I Agree, or Do I: A Rights-Based Analysis of the Law on Children’s Consent in the Digital World, 34(2) Wisconsin International law Journal (2016).

- (iii) The need to prescribe a single threshold to ensure practical implementation.

At the moment, keeping in view the fact that the age for majority in the Contract Act is 18 and the provision of consent for data sharing is often intertwined with consent to contract, the age of 18 is recommended as the age below which a person is classified as a ‘child’ for the purpose of this law. We are aware that from the perspective of the full, autonomous development of the child, the age of 18 may appear too high. However, consistency with the existing legal framework demands this formulation. Were the age of consent for contract to reduce, a similar amendment may be effected here too.

(c) Barred Practices

Certain types of data processing have been objectively found to be harmful for children. Harm, as used here, may be tangible (in terms of physical or reputational harm) or intangible (in terms of loss of autonomy). These include: behavioural monitoring, tracking, targeted advertising and any other type of processing which is not in the best interest of the child.¹⁵² Guardian data fiduciaries must be barred from these practices insofar as it pertains to children.

To identify whether a service is being accessed by a child, the data fiduciary (including the guardian data fiduciary) shall adopt appropriate age verification mechanisms (mandatory login or date of birth input or other approved age verification mechanisms) and carry out processing on the basis of parental consent. An exception to any parental consent requirement would be a guardian data fiduciary that is exclusively engaged in the provision of counselling or child protection services to a child.

(d) Regulatory Approach

As is evident from the above scheme, the law will protect children’s data in the following manner:

For guardian data fiduciaries, when providing services to children, certain types of processing that are harmful will be impermissible. Such data fiduciaries will have to incorporate appropriate age verification mechanisms and parental consent mechanisms.

For data fiduciaries, who are not guardian data fiduciaries, the special obligations (as specifically applicable to guardian data fiduciaries) will not be applicable. Such data fiduciaries will also be required to incorporate appropriate age verification mechanisms and parental consent mechanisms.

¹⁵² Deborah Lupton and Ben Williamson, The datafied child: The dataveillance of children and implications for their rights, 19(5) New Media & Society (2017).

It is important to note that children constitute a large constituency of users of the internet (1/3rd of total internet users).¹⁵³ Since this is the case, a proportionate regulatory response would be to impose a general obligation to process personal data of a child in a manner that is in the best interests of the child. This principle can be developed further through codes of practice, standards and jurisprudence of courts of law.

We believe that the suggested approach is preferable to the current regulatory approach relating to children's data that is based *solely* on a system of parental consent. A dominant criticism against parental consent is that it is prone to circumvention, as it risks encouraging children to lie about their age, without necessarily achieving the intended purpose of protection.¹⁵⁴ Further, an overt reliance on parental consent may take away from the seriousness of the choice made by parents.¹⁵⁵

Motivated by the need to protect children's personal data, we have imposed heightened obligations on guardian data fiduciaries who are barred from certain identified and harmful practices, along with processing permitted on the basis of parental consent. However, the proposed regulatory framework is not closed to incorporating improvements in the parental authorisation regime. These can become a part of the framework through codes of practice, as outlined above, providing greater flexibility in the development of the law to keep pace with technological advancement. The suggested framework sets up a regime that is in the best interests of the child.

IV. Community Data

Community data relates to a group dimension of privacy and is a suggested extension of our data protection framework. It is a body of data that has been sourced from multiple individuals, over which a juristic entity may exercise rights. Such data is akin to a common natural resource, where ownership is difficult to ascertain due to its diffused nature across several individual entities. It is relevant for understanding public behaviour, preferences and making decisions for the benefit of the community.

The difference between community data and other large-scale data collection lies in the degree of involvement of the larger community in building the body of data. It challenges the

¹⁵³ Dorde Krivokapic and Jelena Adamovic, Impact of General Data Protection Regulation on Children's Rights in Digital Environment, Year LXIV(3) Belgrade Law Review 3 (2016) referring to S. Livingstone et al., One in three: internet governance and children's rights, The Global Commission on Internet Governance, Paper Series No. 22 (2015); further, see The State of the World's Children 2017: Children in a Digital World, UNICEF (2017) available at <https://www.unicef.org/publications/index_101992.html> (last accessed on 11 May 2018).

¹⁵⁴ See Milda Macenaitė and Eleni Kosta, Consent for processing children's personal data in the EU: Following in US Footsteps?, 26(2) Information & Communications Technology Law, at p.181. Parental consent, if implemented would also require the law to determine the age when parental consent expires and the individual's consent needs to be taken afresh. Why one particular age may be problematic has been pointed in the context of healthcare research where the child is progressively maturing, see M. J. Taylor et al, When can the child speak for herself? The limits of parental consent in data protection law for health research, Medical Law Review (2017).

¹⁵⁵ Catherine Montgomery & Jeff Chester, Data Protection for Youth in the Digital Age: Developing a Rights-based Global Framework, 4 European Data Protection Law Review (2015).

notion of individual control over her own personal data. Individuals may not be aware of what their data can disclose when aggregated with billions of other data points.¹⁵⁶ For example, Google Maps derives information about drivers' location, speed and itinerary through GPS enabled smartphones of numerous individuals.¹⁵⁷ This data is analysed by algorithms and produces reliable data on traffic flow across the world. Google Maps also collects information on places visited by individuals by asking them specific questions, which helps produce indicators like the availability of parking spots and washrooms, and popular hours at local stores.

Though these services are incredibly useful, two concerns arise. First, an individual's sharing of her personal data (such as current location) may lead to the sharing of similar personal data of her spouse, friends or family, without their consent.¹⁵⁸ Second, juristic entities make use of Big Data and can identify patterns of behaviour. This can have spill-over effects on the entire community as decisions may be taken on the basis of such patterns. Thus, community data may deserve protection.

A suitable law will facilitate collective protection of privacy by including a principled basis for according protection to an identifiable community that has contributed to community data.¹⁵⁹ This will take the form of class action remedies for certain kinds of data breaches involving community data with diffused social and systemic harm.¹⁶⁰ Tools like group communication and sanction may be envisaged. Such protection will take into account any intellectual property ownership of the juristic entity.

We strongly recommend that the Government of India considers such a law. It is our considered view, that not only individuals and communities, but in the near future corporate data too may require specific protection in the digital economy. Though the details of how such developments will take place, and indeed how community data will be protected will develop over time, acceptance of this principle may be seen as a peg on which such future developments may take place.

V. Entities to which the Law Applies

As is apparent from the scheme of this law, preventing privacy harms is essential for a free and fair digital economy. Such harm can ensue from processing by any entity, whether it be a government or a private entity. The ownership or structure of the entity is irrelevant for the purpose of this determination. On the contrary, the data that is processed, the reasons for such processing, and security standards maintained are the critical factors to determine the applicability of the law.

¹⁵⁶ Joshua Fairfield and Christoph Engel, Privacy as a Public Good, 65(3) Duke Law Journal (2015) at p. 390.

¹⁵⁷ Patrick McDeed, The Big Data Driving Google Maps available at <<http://ltd.edc.org/big-data-driving-google-maps>> (last accessed on 22 April, 2018).

¹⁵⁸ See Neil M. Richards, The Dangers of Surveillance, 126 Harvard Law Review (2013) at p. 1939 as cited in Joshua Fairfield and Christoph Engel, Privacy as a Public Good, 65(3) Duke Law Journal (2015) at p. 389.

¹⁵⁹ Joshua Fairfield and Christoph Engel, Privacy as a Public Good, 65(3) Duke Law Journal (2015) at p. 396.

¹⁶⁰ See Article 49, South Korean Personal Information Protection Act, 2011.

The question of whether the law will apply to the government or not is a red herring. It assumed relevance in light of the SPD Rules, which limited its applicability to body corporates. We do not see the reason for such a distinction to persist. Governments, as data fiduciaries, process large amounts of personal data, be it related to taxation, Aadhaar, social security schemes, driving permits, etc. Unlawful processing of such data can cause significant harm to individuals. All jurisdictions that we have considered in detail for our report have included the government; some like the US, have placed greater restrictions on it.

In our context, governments as data fiduciaries must be within the remit of the law. Ensuring that the state respects the right to privacy of the citizen should be a key aim of any data protection framework building on the fundamental right to privacy. In Chapter 1, we discussed the need to create a collective culture which values privacy. The state which collects and processes vast amounts of information of citizens must lead by example, as a data fiduciary, in creating such a culture.

At the same time, it must be recognised that several purposes for state processing of personal data may relate to the public interest. This may include processing for national security, investigating crime, protecting revenue etc.¹⁶¹ Specific purpose-based exemptions for some of these categories must be created within the law. There may be other functions of the state where the relationship between the state and the citizen cannot be equated with that of a contractual relationship between private actors. These issues are dealt with in detail in Chapter 8 of the Report.

¹⁶¹ These four were recognised by Chandrachud, J., in *Puttaswamy*, (2017) 10 SCALE 1.

RECOMMENDATIONS

- The definition of personal data will be based on identifiability. The DPA may issue guidance explaining the standards in the definition as applied to different categories of personal data in various contexts. **[Section 3(29) of the Bill]**
- The law will cover processing of personal data by both public and private entities. **[Sections 3(13) and 3(15) of the Bill]**
- Standards for anonymisation and de-identification (including pseudonymisation) may be laid down by the DPA. However, de-identified data will continue to be within the purview of this law. Anonymised data that meets the standards laid down by the DPA would be exempt from the law. **[Sections 3(3), 3(16) and 61(6)(m) of the Bill]**
- Sensitive personal data will include passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric and genetic data, and data that reveals transgender status, intersex status, caste, tribe, religious or political beliefs or affiliations of an individual. However, the DPA will be given the residuary power to notify further categories in accordance with the criteria set by law. **[Sections 3(35) and 22 of the Bill]**
- Consent will be a lawful basis for processing of personal data. However, the law will adopt a modified consent framework which will apply a product liability regime to consent thereby making the data fiduciary liable for harms caused to the data principal. **[Section 12 of the Bill]**
- For consent to be valid it should be free, informed, specific, clear and capable of being withdrawn. For sensitive personal data, consent will have to be explicit. **[Sections 12 and 18 of the Bill]**
- A data principal below the age of eighteen years will be considered a child. Data fiduciaries have a general obligation to ensure that processing is undertaken keeping the best interests of the child in mind. Further, data fiduciaries capable of causing significant harm to children will be identified as guardian data fiduciaries. All data fiduciaries (including guardian data fiduciaries) shall adopt appropriate age verification mechanism and obtain parental consent. Furthermore, guardian data fiduciaries, specifically, shall be barred from certain practices. Guardian data fiduciaries exclusively offering counselling services or other similar services will not be required to take parental consent. **[Section 23 of the Bill]**
- The principle of granting protection to community data has been recognised by the Committee. This should be facilitated through a suitable law which is recommended to be enacted by the Government of India in the future.

CHAPTER 4: OBLIGATIONS OF DATA FIDUCIARIES

The obligations set out under a data protection law are critical to ensure the twin objectives of limiting processing to the fulfilment of purposes of data principals, while maximising gains from data processing for society at large. Failure to adhere to such obligations provides grounds to hold data fiduciaries accountable.

This chapter outlines the Committee's approach with regard to the various obligations that will be imposed on fiduciaries. Such obligations, many of which have been part of data protection principles since the FIPPs,¹⁶² require careful adaptation with the emergence of new technologies of Big Data processing facilitated by AI and machine learning. While this report does not delve into the benefits and harms of such processing *per se*, it considers their relevance in devising a data protection framework that respects individual autonomy and upholds systemic fairness.

A. White Paper and Public Comments

The White Paper recognised purpose specification and use limitation as means to secure an individual's right to retain control over the manner in which her personal data is collected, used and disclosed.¹⁶³ It was felt that standards would have to be developed to guide data fiduciaries about the meaning of data minimisation in the context of collection and use.¹⁶⁴ While processing for incompatible purposes was considered to be impermissible, keeping in view the multi-functional nature of data, layered privacy notices, which provide further guidance on data use practice, were suggested instead of specifying use in a single privacy notice.¹⁶⁵ It was also recommended that use limitation may be modified on the basis of contextual understanding, therefore subsequent use may be permitted if it was in accordance with a reasonableness standard.¹⁶⁶

A majority of commenters felt that the principles of purpose specification and use limitation were essential to avoid the misuse of personal data. However, opinions varied regarding the degree of alternate uses to be permitted, with some commenters opining that narrow definitions adversely impacted innovation, while others warned against vague and broad

¹⁶² The FIPPs were first laid down in a report by the US Department of Health, Education and Welfare, See Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers and the Rights of Citizens Report (1973) available at <<https://www.justice.gov/opcl/docs/rec-com-rights.pdf>> (last accessed on 7 May 2018).

¹⁶³ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at pp. 109-110.

¹⁶⁴ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at pp. 109-110.

¹⁶⁵ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at pp 109-110.

¹⁶⁶ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at pp. 109-110.

definitions as they failed to provide individuals with meaningful notice and consent. Most commenters believed that the processing of data should be allowed for compatible purposes and the use should be deemed compatible if it is reasonably connected to the overall activity of the data principal collecting such data. Commenters were in agreement with the White Paper's suggestion of a reasonableness standard i.e. processing can happen for purposes that a reasonably informed individual may expect.

The White Paper felt that the principle of storage limitation should find place in Indian law, however it was not feasible to specify precise time limits for storage of data. This would, instead, depend on the purpose for processing.¹⁶⁷ The White Paper also recommended use of terms such as 'reasonably necessary or necessary' to qualify the time period for storage and thereafter issuance of guidelines and court interpretation for clarity in implementation.¹⁶⁸

A majority of commenters agreed with the White Paper's view on incorporating storage limitation. Most commenters believed that the law should contain a standard of reasonable necessity and time limits should be clarified through subsequent guidance. Commenters also suggested that with the advent of Big Data, new purposes may arise and therefore data could either be stored in anonymised form or renewal of consent could be obtained. Further, some commenters suggested that storage limitation not be imposed for meeting obligations of law and processing for historical, statistical and research purposes.

With regard to data quality, the White Paper took the view that it should be incorporated in Indian law. However, it was felt that the burdens imposed on the industry be balanced.¹⁶⁹ Use of terms such as 'reasonably necessary' was suggested to achieve the same.¹⁷⁰ All commenters agreed with the need to maintain data quality. However, most commenters were in favour of imposing the obligation of maintaining accuracy on data principals and felt that it would be an onerous task for the fiduciaries to ensure the same. The commenters also suggested that data principals have the right to correct inaccuracies in their data.

The White Paper was of the view that individuals be notified of data breaches where there was a likelihood of privacy harms being caused as a result of the breaches.¹⁷¹ It was also suggested that the DPA be immediately notified on detection of breach. Further, too short a

¹⁶⁷ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 120.

¹⁶⁸ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 120.

¹⁶⁹ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 120.

¹⁷⁰ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 120.

¹⁷¹ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 165.

time for notifying the breach may be too onerous on small organisations and may prove to be counter-productive since there may be inadequate information about the breach and its likely consequences.¹⁷² The format of the notification could be based on guidance issued by the DPA.¹⁷³ Some commenters were in favour of adopting the definition of personal data breach as provided in the EU GDPR, while others suggested the inclusion of confidentiality, integrity and availability breach in that definition. A large number of commenters were of the opinion that notification to the DPA in case of a breach should be mandatory. Comments with regard to the timeframe of notification varied from a reasonable timeframe to mandatory time spans. A few commenters also opined that notifying the DPA about every breach would overburden it, instead it should only be notified in case of major breaches.

B. Analysis

I. Fair and Reasonable Processing

In a fiduciary relationship, it is essential that the obligations of the fiduciary are clearly delineated. This is a corollary of the basic nature of such a relationship where the principal is dependent on the fiduciary for a particular service or achievement of an objective. The very existence of a fiduciary relationship is premised on the view that the relation between parties, and consequently the fulfilment of the objective by the fiduciary, may lead to an abuse of power.¹⁷⁴ While this may be true in any contract where contracting parties have unequal bargaining power, a fiduciary relationship is characterised by one party's dependence on another for performance of a service or achievement of an objective. Here, the law might deem it particularly necessary to intervene to prevent such abuse.¹⁷⁵ Thus the basic obligations to be followed by data fiduciaries in order to prevent abuse of power must be laid down in law.

All fiduciaries, irrespective of the exact nature of the contractual relation, must uphold trust and loyalty placed in them by the data principal.¹⁷⁶ This takes the form of a duty of care, i.e. to act in the best interest of the principal. Such a duty is mandated in order to ensure that no abuse of power ensues from the unequal nature of the fiduciary relationship.¹⁷⁷

¹⁷² White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 165.

¹⁷³ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 165.

¹⁷⁴ T. Frankel, Fiduciary Law, 71(3) California Law Review (1983) at pp. 809-810.

¹⁷⁵ Examples of fiduciary relationships could range from trustees, administrators and bailees in classical law to corporate directors and partners in the context of modern corporations and partnerships respectively. See T. Frankel, Fiduciary Law, 71(3) California Law Review (1983) at pp. 795-796. Further see, T. Frankel, Fiduciary Law (Oxford University Press, 2011).

¹⁷⁶ Jack M Balkin, Information Fiduciaries and the First Amendment, 49(4) UC Davis Law Review (2016).

¹⁷⁷ Jack M Balkin, Information Fiduciaries and the First Amendment, 49(4) UC Davis Law Review (2016) at pp. 1207-1208.

For a data fiduciary in the digital economy, abuse of power is understood as the data fiduciary processing personal data in a manner not authorised by the principal or law, for ends that may not be in the principal's best interest. The objective of preventing such abuse is best captured by an obligation to ensure fair and reasonable processing.

The obligation to process fairly implies that the data fiduciary must act in a manner that upholds the best interest of the privacy of the principal. Further, the obligation to process reasonably also implies that the processing must be of such a nature that it would not go beyond the reasonable expectations of the data principal. Ensuring fairness and reasonableness in processing are obligations that go beyond simply lawful processing on the basis of one of the grounds laid down in law. Placing such an obligation is recognition of the fact that given the unequal nature of the relationship and its inherent opacity, what is legal may not *ipso facto* be fair or reasonable.¹⁷⁸ Further it is testament to the fact that consent which may be valid for creating legal relationships may not be sufficient to fully disclaim liability.¹⁷⁹

All personal data transfers in our framework must emanate from a legal ground (or a narrowly tailored exemption). For the obligation of fair and reasonable processing to be effective, it should be equally applicable to entities with whom the fiduciary might have shared data for fulfilment of the purpose, irrespective of whether such entity has a direct relationship with the individual or not. This can include data processors whose services may be necessary for carrying out the principal's purposes. Such data processors, who act on behalf of the data fiduciary, owe a similar duty of care to data principals in relation to processing as that owed by the said data fiduciary. This duty is owed regardless of the fact that the data processor does not control the objectives or ends of the processing and is only given a mandate by the data fiduciary.

Needless to say, the extent of the obligations of a data processor may differ, depending on the exact nature of processing in question and the requisite duty of care may be duly reflected in the contract between the data fiduciary and itself. This is precisely why laying down such a general principle of fair and reasonable processing will allow it to be developed by the DPA and courts of law, taking into account technological developments over time and differential obligations of different entities.

II. Purpose Limitation and Data Minimisation

¹⁷⁸ For instance, standard form contracts on the internet are an example, which while legal, may not always be fair due to the slim likelihood of the consumers reading and understanding the terms. See Robert A. Hillman, Consumer Internet Standard Form Contracts in India: A Proposal, 29(1) National Law School of India Review (2017).

¹⁷⁹ HLA Hart, The Ascription of Responsibility and Rights, 49 Proceedings of the Aristotelian Society (1949). See also Mindy-Chen Wishart, Undue Influence: Vindicating Relationships of Influence, 59(1) Current Legal Problems (2006).

Having established the general obligation on all fiduciaries, specific provisions to prevent abuse of power require detailing. To do this, the exact nature of legal relationships in the data economy need to be understood. The basic relationship is between two persons — the data principal and the data fiduciary. In this relationship, the data principal entrusts the fiduciary with personal data to achieve a particular purpose. This may involve, for instance, entrusting financial information to complete a transaction. The fiduciary undertakes to fulfil the purpose, whether itself or with the assistance of third parties. This relation, between ‘principal and ‘fiduciary’ occurs at a mammoth scale in the data economy with over 16.1 zettabytes of data being generated in 2016.¹⁸⁰

At its core, each relation between data principal and data fiduciary is undergirded by elements which characterise a classic fiduciary relationship: a data principal (data subject) entrusts personal data to a data fiduciary (data controller) for a particular purpose (financial transaction). If abuse of power is to be prevented, it is critical that the data fiduciary is obliged to use the personal data entrusted to it by the data principal only for the purpose for which the principal reasonably expects it to be used. This is the germ of the collection and purpose limitation principles. Both these principles seek to achieve the goal of data minimisation, as described in the White Paper.¹⁸¹

The purpose limitation principle has been the bedrock of data protection regimes for the last three decades.¹⁸² It contains two sub-principles: first, that the purpose for which the personal data is processed must be clearly specified to the data principal (purpose specification); second, the processing must be limited to such purposes, or other compatible purposes (use limitation). Implicit in each of these sub-principles are two assumptions: first, that specification of purpose must meet a certain standard of specificity — simply specifying purposes in a vague manner will not be sufficient. Second, any unspecified use will be determined from the point of view of whether the processing is fair and reasonable in light of the purpose that was specified.

The first assumption is questionable. That purposes can be laid down with any degree of specificity is belied by existing practice in consent forms. By stating that the purposes for processing are ‘improving consumer experience’, ‘for better services’, etc. the principle is facially, though not substantively met. Yet, these may be valid, legitimate and lawful purposes. Further detailing of purposes in the interest of informing consent-giving, as is done

¹⁸⁰ It is estimated that by 2025 world’s data will reach 163 zettabytes. It must be noted that not all data is personal data; see David Reinsel et al., Data Age 2025: The Evolution of Data to Life-Critical available at <<https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf>> (last accessed on 7 May 2018).

¹⁸¹ “The underlying logic of the use limitation and purpose specification principles is that of data minimisation, or the practice of limiting the collection of personal information to that which is necessary to accomplish a specified purpose”. White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at pp. 105-106.

¹⁸² For instance, see the EU GDPR, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013), FIPPs (FTC, US).

by several data fiduciaries, might lead to long and unreadable consent forms, becoming counter-productive.¹⁸³ We are caught between the rock of vagueness and the hard place of incomprehensibility in trying to arrive at an appropriate standard of specificity.

Further, a limited set of future uses could be allowed to provide some degree of flexibility to the data fiduciary. This is based on the salient realisation that there may be other potentially beneficial uses of data which would not directly be at odds with the purpose specified to the data principal. Critically, such uses should be compatible, which has been understood to mean upholding the requirement of fairness.¹⁸⁴ The flexibility offered by this principle would permit use of the personal data for any other purpose by the data fiduciary which the data principal would reasonably expect having regard to the context and circumstances of processing of personal data. This is a commonsensical proposition, implemented by relating such uses back to the original purpose specified.

The purpose limitation principle is usefully seen in conjunction with another general principle, that of collection limitation. The principle of collection limitation mandates that only such data should be collected that is necessary for achieving the purposes specified for such processing. Thus, the minimum data necessary for achieving a purpose could be collected, and such data used only for the specified purpose and other compatible purposes and no other. Taken together, these are designed to lead to data minimisation that in turn, allows greater granular control for the data principal.

III. Big Data Challenges to Data Minimisation and Purpose Limitation

This belief of control through minimisation is a far cry from existing practice. Apart from the practices of vague purpose specification described above, the digital economy operates, not on the principle of data minimisation, but rather its antithesis, data maximisation.¹⁸⁵ This is particularly the case with the emergence of Big Data, processing vast amounts of data at scale to discern patterns of individual behaviour or market trends.¹⁸⁶ This is made possible by algorithms that enable machines to process at scale, learn from such processing, remember their learnings to gain intelligence and analyse such learnings constantly to generate useful results. These results are then used to more precisely target products, services, interventions to audiences now identified as receptive. Needless to say, such results are probabilistic,

¹⁸³ For instance, Gmail's privacy policy is a nine-page document that details the various purposes for which the data can be processed. See Google, Privacy Policy (2017) available at <https://static.googleusercontent.com/media/www.google.com/en/intl/en/policies/privacy/google_privacy_policy_en.pdf> (last accessed on 6 May 2018).

¹⁸⁴ UK Information Commissioner's Office, Big Data, artificial intelligence, machine learning and data protection available at <<https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>> (last accessed on 6 May 2018) at p. 37.

¹⁸⁵ O. Tene and J. Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11(5) Northwestern Journal of Technology and Intellectual Property (2013) at p. 242.

¹⁸⁶ Big Data is characterised by three Vs, namely 'volume' which refers to massive databases, 'velocity' which refers to real time data and 'variety' which relates to different sources of data. See White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 8.

though their widespread use in the digital economy perhaps suggests that they are more often right than wrong.

Big Data processing is widely understood as comprising four stages: first, data collection from volunteered, observed, inferred or legally mandated data sets. This may or may not be limited to personal data sets; second, its storage and aggregation at scale; third, analysing such aggregated data through machine learning; fourth, its use for prediction or targeting.¹⁸⁷ Through these four stages, it is evident that data that is processed as well as the results from such data, may or may not relate to identified individuals. For example, Big Data analytics is widely used to predict weather patterns on the basis of large-scale processing of weather statistics as well as other relevant information.¹⁸⁸ At the same time, it is widely used in order to target products to particular individuals on the basis of their preferences derived from analysis of a large volume of diverse data sets.¹⁸⁹ Such targeting can be immensely useful - predictive text on searches brings down time spent on searches, responsive medical intervention ensures quicker emergency care¹⁹⁰ and tracking student performance and related data helps prevent dropouts.¹⁹¹ Equally, Big Data analytics may also lead to tangible harms to individuals when targeting goes awry. Since the nature of Big Data analytics is probabilistic, incorrect targeting may lead to inaccuracy of personal data, ensuing denial of service and discrimination. Examples of such harms abound.¹⁹²

An assessment of the relative benefits and harms of Big Data processing is orthogonal to our report. The benefits of such processing must outweigh its harms for such processing to become widely accepted and used by fiduciaries. That appears to be the case. Tim Wu writes about how the business model of the entire digital economy appears to be founded on free services and the use of personal data for targeted advertising.¹⁹³ It need not have turned out

¹⁸⁷ International Working Group on Data Protection in Telecommunications, Working Paper on Big Data and Privacy, Privacy principles under pressure in the age of Big Data analytics (2014) available at <https://www.datenschutz-berlin.de/pdf/publikationen/working-paper/2014/06052014_en.pdf> (last accessed on 6 May 2018) at pp. 4-5.

¹⁸⁸ UK Information Commissioner's Office, Big Data, artificial intelligence, machine learning and data protection available at <<https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>> (last accessed on 6 May 2018) at p. 10.

¹⁸⁹ Orcan Intelligence, Big data analytics is used by companies such as Netflix to adjust content and personalize the user-experience, see How Netflix uses Big Data (2018) available at <<https://medium.com/swlh/how-netflix-uses-big-data-20b5419c1edf>> (last accessed on 6 May 2018).

¹⁹⁰ According to recent research, data from fitness trackers could help predict the risk of a heart-attack, see S. Davila et al, Beyond Fitness Tracking: The use of consumer-grade wearable data from normal volunteers in cardiovascular and lipidomics research, PLoS Biol 16(2): e2004285.

¹⁹¹ See D. West, Big Data for Education: Data Mining, Data Analytics, and Web Dashboards, Brookings (2012) available at <<https://www.brookings.edu/wp-content/uploads/2016/06/04-education-technology-west.pdf>> (last accessed on 06 May 2018).

¹⁹² For instance, the insurance company Progressive required customers to install a monitoring device in their cars through which customers who drove infrequently and avoided driving during the night were given better rates on the basis of the assumption that such driving practices reduced the risk of accident. However, this ended up discriminating against late-night shift workers who were largely from minority communities. For further reading see The Center of Internet and Society, Benefits and Harms of "Big Data" (2015) available at <<https://cis-india.org/internet-governance/blog/benefits-and-harms-of-big-data>> (last accessed on 6 May 2018).

¹⁹³ This is described as nano-targeting. Tim Wu, The Attention Merchants: The Epic Scramble to get Inside Our Heads (Vintage Books, 2016) at p. 296-302.

this way and need not continue this way if significant harms ensue as a result of erroneous targeting. It is a choice that businesses have made, and individuals have consented to, if not positively supported. This is neither the time nor place to question this development, except to retain a healthy scepticism of whether a “free internet” is, or will remain, welfare-maximising for individuals.

For the purposes of a data protection framework, Big Data processing presents a frontal challenge to the well-established principles of collection limitation and purpose limitation. The basis for processing at scale is the collection of large amounts of personal data and its subsequent use for a variety of purposes. Particularly, the challenges are twofold: first, the uses to which personal data are put often only become apparent over time. This is because several uses are derived only after an assessment of the personal data from a collection of data sets from different sources, which may not have been intended to be combined.¹⁹⁴ As a White House Report on Big Data and Privacy¹⁹⁵ notes even the algorithm that is used to process such data resulting in potential future uses may not be in existence at the time of initial collection. Second, these uses may be a result of re-identification of individuals from anonymous data sets. The increasing ease of re-identification means that at the time personal data was collected and notice was provided on uses, such future uses based on re-identification could not have been envisaged.¹⁹⁶ Thus limiting collection is antithetical to large-scale processing; equally, meaningful purpose specification is impossible with the purposes themselves constantly evolving.

In order to ensure that any such use of big data analytics is narrowly tailored and geared towards maximising individual benefits and minimising harm in the digital economy, it is necessary to constrain its uses in ways that optimally respect individual autonomy in a free and fair digital economy. This is possible in the following three ways:

First, to the extent possible, anonymised data can be used which cannot later re-identify an individual. This ensures that the benefits of Big Data processing can continue together with the protection of individual autonomy.

Second, Big Data processing that is used to improve the provision of the service or purposes reasonably expected by the principal, should be permitted to continue. There is no adverse effect on autonomy by the use of a technique (large scale data processing), on the contrary, such use may well be within the reasonable expectation of the principal and presumably for her benefit.

Third, when Big Data processing is used for repurposing, with unknown future purposes which could not have been reasonably communicated to the data principal at the time of

¹⁹⁴ Nancy King and Jay Forder, Data analytics and consumer profiling Finding appropriate privacy principles for discovered data, 32(5) Computer Law and Security Review (2016) at pp. 699-700.

¹⁹⁵ Executive Office of the President, President’s Council of Advisors on Science and Technology, US, Big Data and Privacy: A Technological Perspective (May 2014) at p. ix.

¹⁹⁶ Nancy King and Jay Forder, Data analytics and consumer profiling Finding appropriate privacy principles for discovered data, 32(5) Computer Law and Security Review (2016) at p. 704.

collection, then collection limitation and purpose specification might not be possible in the form in which it is set out in the law. Narrow tailoring of the use of personal data requires the following substantive conditions to be met:

- (i) Personal data should not be processed in a manner that gives rise to a risk of significant harm to any data principal. This ought to function as a general obligation on any fiduciary that engages in any repurposing according to subsequent purposes that could not be reasonably communicated at the time of collection.
- (ii) Personal data may be processed in a manner that does not take any decision specific to, or action directed specifically at, any individual. This can take the form of analysis of general trends or patterns. Since there is no possibility of individual harm which flows from such usage, it should be permitted to continue. Processing subject to this condition has been discussed further in Chapter 8 under ‘Research Activities’.
- (iii) If, however, personal data is used to take any decision specific to, or action directed specifically at any individual, then explicit consent of the individual in accordance with the law is to be taken. This is necessary to uphold individual autonomy such that any use of personal data to take any action that impacts a data principal must be processed on the basis of her consent. Further, for any data fiduciary who wishes to engage in such processing, certain organisational obligations must be adopted. These include, but are not limited to, a data trust score, regular data audits, a DPO and a transparent mechanism for data processing which allows the individual access at any time to the personal data held by a fiduciary with an option to correct such personal data for inaccuracies.

It may be argued that seeking such consent may be un-implementable. We do not see why this must be the case — if an individual can be targeted precisely for the purpose of showing her an advertisement or a particular communication, surely, she can be targeted for seeking consent before such action. The final call on how the consent should be obtained should be left to the determination of the DPA.

Such repurposing should only be permitted if such later purposes could not have been known at the time of collection and could not reasonably be communicated to the individual. If such knowledge of purpose is objectively possible and necessary communication of the same to the individual has not been done, such initial processing should be made unlawful and appropriate enforcement action may be taken by the DPA.

It is our view that in this manner, the interests of individual autonomy can be optimally protected in creating a free and fair digital economy. The above discussion is in the nature of recommendations to the Central Government which may be taken up at an appropriate time.

IV. Transparency

In securing their rights under data protection law, a prime barrier faced by data principals is the lack of information on how their personal data comes to be processed. Especially in the digital context, it becomes difficult for a data principal to know and understand whether, by whom and for what purpose personal data about her is being collected and processed.¹⁹⁷ In this regard, it is essential that processing be carried out transparently. This not only bolsters the fairness of the processing activities, ensuring that data principals can trust them, but also makes sure that data fiduciaries are accountable by creating some scope for principals to challenge them.¹⁹⁸

As a result of this, a principle of transparency is incumbent throughout the life cycle of a data processing activity from the time the data is collected to various points in the interim. It has thus been integrated into our proposed framework at various points. Most prominently, a data fiduciary is obliged to provide *notice* to the data principal no later than at the time of the collection of her personal data. If the data is not being collected from the principal directly, this obligation is still applicable, and the fiduciary must provide the notice as soon as is reasonably practicable. The information that a fiduciary is required to disclose to the data principal has been specified to ensure that it alleviates, as best as is possible, the problems of opacity, uncertainty, lack of clarity, and lack of accountability because of which privacy harms are caused. Not only must the data principal be informed as to who is processing what personal data of theirs for what purposes, they must also be told various points of relevant information including the basis of processing, their ability to withdraw consent (if processing is based on consent), any legal obligations on the basis of which the processing is taking place, persons with whom the data may be shared, the period of retention of data, as well as the procedure for the exercise of data principal rights, the procedure for grievance redressal and the right to file complaints with the DPA.

These points of information must be conveyed to the principal in all circumstances except where processing is taking place for emergency situations requiring prompt action. It must also be ensured that the form of the communication is clear and concise so that it is easily comprehensible. There may also be various situations where it is necessary for the information to be communicated in multiple languages.

¹⁹⁷ Recital 58, EU GDPR (identifying the “proliferation of actors and the technological complexity of practice” as being especially problematic reasons for such difficulty).

¹⁹⁸ Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679 (2018) at p.5.

Transparency requirements may also be seen in various obligations regarding the manner in which the data fiduciary is to communicate with the data principal in relation with the exercise of any of the data principal's rights (described in Chapter 5). Thus, for instance, the fiduciary is required to acknowledge receipt of requests for the exercise of such rights and clearly communicate adequate reasons for the refusal of any right. Apart from this, the data fiduciary is also required to maintain transparency regarding its general processing activities and practices, making available such information for any data principals seeking clarity on the same at any point of time. This obligation to publicise general practices regarding data processing may be seen as a practice that some entities already follow in the form of organizational privacy policies that may be available on their websites or otherwise placed in prominent locations.

V. Organisational Obligations on Data Fiduciaries

This report has thus far been based on the premise that a free and fair digital economy is possible when the individual, whose personal data is at the core, is the key lever for all data transfers. We are cognisant that such vision is remote from the functioning of the digital economy today where the individual is only notionally in control of her own personal data. Thus, trust in data fiduciaries, particularly today, requires such fiduciaries to take certain organisational measures to ensure that personal data is processed lawfully, fairly and reasonably and not wait for individuals to *ex post* identify non-compliance.

In academic literature, such organisational measures have been described as involving the setting up of an accountability framework for data fiduciaries.¹⁹⁹ In our view, organisational measures are critical components to ensure that data fiduciaries fulfil their obligation of fair and reasonable processing and are in a position to demonstrate such fulfilment when called upon to do so. The enforcement of such obligation may either take place by an assertion of individual right, or, through appropriate audit mechanisms and regulatory action.

This framework has been implemented within a rights-based approach in the EU GDPR. The EU GDPR imposes an accountability obligation that requires data controllers to comply with all obligations under EU GDPR and be able to demonstrate this compliance.²⁰⁰ This requires the implementation of concrete organisational measures to operationalise data protection principles. It is our view that a general obligation to undertake organisational measures to ensure fair and reasonable processing needs to be placed on all data fiduciaries.

¹⁹⁹ In a consent-based framework the data principal is responsible for being aware of the terms of the data access to which she has consented to as opposed to an accountability model where the burden of compliance with obligations is imposed on the fiduciary by the regulator. See Rahul Matthan, Beyond Consent: A New Paradigm for Data Protection, The Takshashila Institution (2017) available at <<http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf>> (last accessed on 6 May 2018); Further see Comments submitted in response to the White Paper by The Takshashila Institution on 30 January 2018 available on file with the Committee.

²⁰⁰ The Article 29 Data Protection Working Party recommended the inclusion of the principle of accountability in the European Union's data protection regime, see Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability (2010). Further, see Article 5(2), EU GDPR.

Regarding the content of such organisational measures, it is our view that they should be carefully calibrated to the nature of the processing which takes place. Thus, for all data fiduciaries, baseline minimum obligations need to be imposed. These include implementation of appropriate security measures and mechanisms for individuals to access their personal data. For significant data fiduciaries, heightened organisational measures need to be taken. These organisational measures have broadly been described as ‘privacy by design’ that establishes data handling practices in the organisation in a manner ensuring compliance with the law by minimising or eliminating adverse impacts on privacy.²⁰¹ This may also ensure cost effective compliance with the obligations under the law. For instance, the EU GDPR refers to the adoption of technical and organisational measures that take into account the rights of individuals while designing policies to ensure that they can effectively meet their obligations under the data protection law.²⁰² A list of such practices, which we hope will develop further through codes of practice, has been devised and submitted to us.²⁰³ We urge the DPA to consider these and other best practices to lay down precise obligations for data fiduciaries so as to ensure strict compliance with the law. In this exercise, it is recommended that the DPA conduct capacity building exercises to create skilled professionals in order to implement a ‘design-thinking’ approach. Industry bodies can also play a pivotal role by assisting the DPA in this process.

A critical obligation which requires specific highlighting here is access control obligation. Access control obligations are designed to ensure that all data accesses are legitimate and that they do not violate consent, purpose limitation or any other substantive provision. This will require all data processing and access requirements to be scrutinised *apriori* and *ex post* through audits. The data fiduciary and any associated processors should maintain non-repudiable logs (perhaps in a blockchain) of all requests and approvals. It must be ensured that data access is according to the authorisations granted. *Ex post* audits are, in any event, possible.

VI. Storage Limitation

The principle of storage limitation, which is closely connected to the principle of purpose limitation, envisages that data should be stored by the fiduciary only for a time period that is

²⁰¹ The principles of ‘privacy by design’ were developed by the Privacy Commissioner of Ontario, Canada and focus on making privacy assurance an organization’s default mode of operation, see Privacy Commissioner of Ontario, Canada, Privacy by Design (2009) available at <<https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf>> (last accessed on 7 May 2018).

²⁰² Recital 78, EU GDPR.

²⁰³ Email Response submitted in response to the White Paper by the Centre for Information of Policy Leadership on 30 January 2018, available on file with the Committee. There are also numerous examples of sector-specific codes of practice, for instance See UK Information Commissioner’s Office, The Employment Practice Code available at <<http://www.pdpjournals.com/docs/99007.pdf>> (last accessed on 12 May 2018); German Data Protection Principles for Connected Vehicles (Vehicles connected to the internet) (2014) available at <<http://www.pdpjournals.com/docs/99009.pdf>> (last accessed on 7 May 2018) etc.

necessary to fulfil the purpose for which it was collected.²⁰⁴ Once the purpose has been achieved, the data should be deleted or anonymised. The rationale behind this is that once processing is over, control over the data may be lost, since it is no longer of any interest to the data fiduciary, which may expose the data to the risk of theft, unauthorised copying or the like.²⁰⁵

In order to avoid any risk of unauthorised access once processing has ceased, the principle of storage limitation will be applicable as an obligation on data fiduciaries. Thus, data fiduciaries will only be able to retain personal data as long as it is required to satisfy the purpose for which it was collected. Thereafter, the said data may be anonymised or erased permanently to meet the requirements of the law. The key requirement is that once the object of processing has been achieved, the data, if retained, should not be capable of identifying any individual.²⁰⁶

The Committee is conscious that such a requirement may impose a compliance burden on fiduciaries in terms of a periodic review of all personal data retained by them. However, such review is necessary to make fiduciaries conscious of the personal data in their possession so that they can act, in a timely manner, to avoid any future breaches. The only exception to the principle of storage limitation would be instances where legal or sectoral or regulatory requirements may necessitate the storage of such personal data for further periods. For, instance the Know Your Customer Guidelines issued by the RBI require that information pertaining to the identification of the customer is to be retained for five years even after the closure of the account.²⁰⁷ These must have overriding application.

Further, as long as the personal data is retained by the data fiduciary, it will be liable for all obligations that are imposed on it by the data protection law. The obligations will continue till the data has either been erased permanently or has been anonymised by the fiduciary. Therefore, obligations would continue to apply even after processing has ceased, as the data retained by the fiduciary remains capable of identifying individuals thereby qualifying as personal data.

²⁰⁴ OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013) available at <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotecti...> (last accessed on 1 May 2018).

²⁰⁵ OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013) available at <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotecti...> (last accessed on 1 May 2018).

²⁰⁶ A key exception to this principle would however probably be processing for research purposes which has been discussed in Chapter 8.

²⁰⁷ RBI, Master Direction – Know Your Customer (KYC) Direction, 2016 available at <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/18MDKYCD8E68EB13629A4A82BE8E06E606C57E57.PD> (last accessed on 1 May 2018) at para 46.

VII. Data Quality

The principle of data quality implies that the personal data being used should be relevant to the purpose for which it is to be used and should be accurate, complete and kept up-to-date.²⁰⁸ The requirements of accuracy, completeness and up-to-dateness are also linked to purpose and therefore should meet the requirements of the purpose for which the personal data was collected. Thus, in the case of studies that rely on longitudinal research, if the data does not meet the three requirements, then the processing of such data may not achieve the desired purpose and in fact may also lead to harm to the data principals.²⁰⁹

Accuracy, completeness and up-to-dateness of data are the key requirements of data quality. Personal data is intrinsically linked to individuals, who are therefore the most reliable source of data. The primary responsibility to provide accurate data to the data fiduciary will rest on the data principal. However, there is a corresponding obligation to ensure that data is complete, i.e. it will satisfy the purpose for which it was collected on the data fiduciary who is collecting such data.

In instances where personal data has been collected from parties other than the data principal, then the obligation would be on the data fiduciary to ensure accuracy, and in case of data being inaccurate, it is corrected, completed or updated upon request by the data principal. This is in conjunction with the right to correction, etc. which has been provided under our law to all data principals.²¹⁰

Further, there will be a general obligation on the data fiduciary to ensure that the personal data being processed is accurate and to ensure that any onward disclosure or sharing of such data to third parties meets the requirements of accuracy. Where keeping the personal data up-to-date is necessary for the purpose of processing, such as in instances where the purpose relies on data remaining current, the fiduciary will be under a general obligation to take necessary steps to ensure that the data is kept up-to-date over time.²¹¹

VIII. Notification for Data Breach

(a) Need for Data Breach Notification

²⁰⁸ OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013) available at <<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldatal.html>> (last accessed on 1 May 2018).

²⁰⁹ OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013) available at <<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldatal.html>> (last accessed on 1 May 2018).

²¹⁰ This has been dealt with in Chapter 5 of this report.

²¹¹ UK Information Commissioner's Office, Guidance on Data Quality available at <<https://ico.org.uk/for-organisations/guide-to-data-protection/principle-4-accuracy/>> (last accessed on 7 May 2018).

With large amounts of data being held by fiduciaries, the breach of personal data becomes a real possibility. A breach can have deleterious consequences for individuals whose personal data has been subject of the breach. Therefore, it becomes important to inform data principals about such instances so that they can take suitable measures to shield themselves from their harmful consequences. However, due to considerations of adverse publicity and avoidance of liability, fiduciaries may be dis-incentivised from reporting incidents of breach to individuals. Thus, a notification to the DPA upon the occurrence of a breach has been envisaged, in keeping with trends in other jurisdictions,²¹² before a notification to the individual is made. It may be noted that such personal data breaches that are subject to obligations of notification should not be confused with breaches of data protection law generally.

(b) What constitutes a Personal Data Breach?

The definition of personal data breach will be structured in a manner that accounts for the three key principles of information security i.e. confidentiality, integrity and availability.²¹³ These principles offer the most holistic understanding of breach and comprehensively cover all the possible facets of a breach. Confidentiality breach implies an unauthorised or accidental disclosure of, or access to, personal data.²¹⁴ Integrity breach constitutes an unauthorized or accidental alteration of personal data.²¹⁵ An availability breach occurs when there is an accidental or unauthorised loss of access to, or destruction of, personal data.²¹⁶ A particular breach may however not fit neatly into any of these categories but may be combination of these. The significant elements of the definition of personal data breach would be the occurrence of ‘disclosure’ or ‘access’, ‘alteration’, and ‘loss of access’ or ‘destruction’ of personal data which occurs in manner that is either ‘accidental’ or ‘unauthorised’.

It is also important to keep in mind that every security incident may not qualify as a personal data breach. Only security incidents that affect the confidentiality, integrity and availability of personal data, thereby compromising the data fiduciaries’ ability to comply with the various requirements of data protection law will qualify as personal data breaches mandating notification.

²¹² For example, Article 33(1), EU GDPR, Section 6, New Mexico Data Breach Notification Act, 2017.

²¹³ The fundamental principles of information privacy have been dealt in detail in our White Paper, see White Paper of the Committee of Experts on a Data Protection Framework for India available AT <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 161.

²¹⁴ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 161.

²¹⁵ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 161.

²¹⁶ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 161.

(c) When does it need to be notified to the DPA?

A personal data breach may be of varying degrees of severity. For instance, an unauthorised hack of personal data held by a financial services company as well as the accidental deletion of contact details of members maintained by a social club, while both falling within the definition of personal data breach are not breaches of equal gravity. While the former, due to the possibility of significant harm to data principals, merits notification to the DPA the latter does not. In order to avoid the notification of relatively benign breaches of personal data, only such breaches will have to be notified that pose a likelihood of harm to the rights of data principals.

The Committee is cognisant that a notification requirement which depends on harmful consequences to the rights of the data principals may not afford sufficient clarity to fiduciaries. However due to the complicated nature of breaches it also not advisable to list specific thresholds in the law. It is therefore envisaged that the DPA will offer suitable guidance on what action is necessary to be taken.

The content of such notification should at the minimum include the nature of personal data that has been subject to breach and the number of individuals who have been affected by the breach, the possible consequences of the breach and the measures being taken to contain the breach.²¹⁷

After becoming aware of such a breach, the fiduciary will be required to comply with the notification requirement as soon as possible. The obligation is being envisaged as a layered one where the fiduciary will be required to be in continuous communication with the DPA regarding the measures being taken to identify the scope and extent of the breach and the procedures being adopted to contain the breach. Though the obligation is to notify the DPA as soon as the circumstances surrounding the breach permit the fiduciary to do so, an outer limit for such notification should nonetheless be set so as to prevent risk of misuse.

(d) When does it need to be notified to individuals?

Upon notification, the DPA shall have the power to decide the severity of the breach and if relevant, the manner in which it needs to be reported to the individuals whose data has been breached. The breach should be notified to the individuals in instances where such a breach not only poses harm to the data principals, but also where some action is required on part of the principals to protect themselves from the consequences of the breach. The DPA has been granted the powers to determine when and how such notification is required to prevent the fiduciary from making a unilateral decision in this regard which may be motivated by factors other than best interests of the data principals. Further, the DPA is expected to better guide the actions of the data fiduciary and suggest or direct remedial measures, and it must be ensured that liability for the breach is suitably accorded in an adjudication action.

²¹⁷ Provisions on compensation may apply in such cases, see Chapter 9 of this report.

Failure to notify a breach would make the fiduciary liable to penalty under the provisions of the data protection law.

IX. Data Security

While the basis of a data protection law is the individual's right to informational privacy, obligations securing data protection need to be supplemented by implementation of security safeguards to ensure data security. According to the OECD principles²¹⁸ such security safeguards include physical measures, organisational measures (such as authority levels for accessing data) and informational measures (such as continuous threat monitoring).

The obligation to ensure data security is thus incorporated by the EU GDPR, which adopts the principles of information security requiring the integrity and confidentiality of personal data to be maintained at all times. Thus, personal data should be processed in a secure manner, ensuring that there is no unauthorised or unlawful processing and such data does not suffer from accidental loss or destruction.²¹⁹ Appropriate technical or organisational measures are required to be adopted to ensure data security.

Organisational measures include the application of information security policies in organisations handling data, business continuity plans in the event of breach, controlling access to data within the organisation etc.²²⁰ Technical measures on the other hand include measures of physical and computer or information technology security. These would include adequate physical security of the premises, proper disposal systems for paper and e-waste etc.

Currently, in India the SPD Rules which have been issued under Section 43A of the IT Act²²¹ deal with data security. Rule 8 of the SPD Rules²²² defines reasonable security practices as implementation of security practices and standards, a comprehensively documented information security programme, and information security policies that contain managerial, technical, operational and physical security control measures commensurate with the information assets being protected and the nature of the business. The IS/ISO/IEC 27001 international standard is a recognised standard under the SPD Rules. Industry associations or entities which follow their own standards have to get them approved and notified by the Central Government.

²¹⁸ OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013) available at <<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotecti onofprivacyandtransborderflowsofperson aldata.htm>> (last accessed on 1 May 2018).

²¹⁹ Article 5(1)(f), EU GDPR.

²²⁰ UK Information Commissioner's Office, Guidance on Data Security, available at <<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/>> (last accessed on 07 May 2018).

²²¹ Section 43A, IT Act.

²²² Rule 8, SPD Rules.

With the introduction of a range of new rights and obligation under the data protection law however, the law will also have to re-emphasise the need for data security measures. The law will set out the general principle that fiduciaries in designing their security policies should ensure the confidentiality, integrity and accessibility of data at all times through organisational and technical measures keeping in mind the purpose and risk posed by their processing. The specificities of what security measures would meet the standards set by the law would be a sector-wise determination and require consultation between the DPA, sectoral regulators and industry bodies. These would be in conjunction with the organisational requirements that have been set out above.

Broader obligations of data security and organisational measures are intended to complement more specific obligations such as data minimisation, data quality, breach notification and storage limitation. Ultimately, the obligation of fair and reasonable processing will be overarching and underline and inform all other obligations. The Committee is of the view that the obligations which have been outlined above will ensure that processing of data occurs in a fair and reasonable manner. Further, they will ensure that any possibility of abuse in the envisaged fiduciary-principal relationship is mitigated, thereby upholding the best interest of the individual in a free and fair digital nation.

RECOMMENDATIONS

- The relationship between the “data subject” and the “data controller” is to be reformulated as a fiduciary relationship between the “data principal” and the “data fiduciary”. **[Sections 3(13) and 3(14) of the Bill]**
- All processing of personal data by data fiduciaries must be fair and reasonable. **[Section 4 of the Bill]**
- The principles of collection and purpose limitation will apply on all data fiduciaries unless specifically exempted. **[Sections 5 and 6 of the Bill]**
- Processing of personal data using big data analytics where the purpose of the processing is not known at the time of its collection and cannot be reasonably communicated to the data principal can be undertaken only with explicit consent.
- A principle of transparency is incumbent on data fiduciaries from the time the data is collected to various points in the interim. Most prominently, a data fiduciary is obliged to provide notice to the data principal no later than at the time of the collection of her personal data. **[Sections 8 and 28 of the Bill]**
- There shall be obligations of data quality and storage limitation on data fiduciaries. However, the responsibility to ensure that the personal data provided is accurate will rest on the data principal. **[Sections 9 and 10 of the Bill]**
- There will be a provision of personal data breach notification to the DPA and in certain circumstances, to the data principal. **[Section 32 of the Bill]**
- Data security obligations will be applicable. **[Section 31 of the Bill]**

CHAPTER 5: DATA PRINCIPAL RIGHTS

In order to ensure a robust data protection law, it is essential to provide data principals with the means to enforce their rights against corresponding obligations of data fiduciaries. These rights are based on the principles of autonomy, self-determination, transparency and accountability so as to give individuals control over their data, which in turn is necessary for freedom in the digital economy. Specifically, some of these rights can be said to flow from the freedom of speech and expression and the right to receive information under Article 19(1)(a) and Article 21 of the Constitution.²²³

The Committee believes that a strong set of data principal rights is an essential component of an empowering data protection law. This chapter discusses the need, scope and implementation of three groups of rights as delineated in the White Paper. The first group consists of the rights to access, confirmation and correction; the second group consists of the rights of objection to processing, objection to direct marketing, objection to decisions made solely by automated processing, data portability and restriction of processing; and finally, the third group which deals with the standalone right to be forgotten.

A. Access, Confirmation and Correction

I. White Paper and Public Comments

The provisional views of the White Paper are that the right to seek confirmation, access and rectification should be incorporated in the data protection law.²²⁴ However, the challenges in the implementation of these data principal rights, particularly relating to their expense and implementation, have been recognised. In this light, the White Paper suggests that a reasonable fee may be imposed by the organisations as determined by a DPA.²²⁵

²²³ The freedom to know has been upheld in the cases of Reliance Petrochemicals Ltd v. Proprietors of Indian Express, AIR 1989 SC 190 at para 34; The State of U.P. v. Raj Narain, AIR 1975 SC 865 at para 74; S.P. Gupta v. Union of India, AIR 1982 SC 149 at para 66. The right to impart and receive information was discussed in The Secretary, Ministry of I&B v. Cricket Association of Bengal, AIR 1995 SC 1236 at para 124 (ii).

²²⁴ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 18 April 2018) at p. 127. The White Paper concludes that, “The right to seek confirmation, access and rectify personal data allow an individual control over data once such data has been collected by another entity. These rights may be suitably incorporated. However these rights are harder to enforce in the context of personal information that has been derived from the habits and observed behaviour of the individual and other such inferred insights. This information is nevertheless personal and an individual should be made aware of the fact that the data fiduciary has this sort of information.”

²²⁵ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 18 April 2018) at p. 127. The White Paper concludes that, “Given that responding to individual participation rights can be costly for organisations, and comes with its set of technical challenges, a reasonable fee may be imposed on individuals when exercising these rights. This will also discourage frivolous and vexatious requests. The fees may be determined via sector specific subsidiary legislation or regulations. An illustration of this is the CIC Act under which the charge for accessing a copy of a person's credit information report by a specified user is laid down by the RBI via regulations.”

Commenters have largely expressed support for the existence of the bundle of data principal rights discussed in the White Paper, namely the rights to confirmation, access and rectification. Several commenters have called for a wide scope for these rights, as the data belongs to the data principals and is being used by entities largely for commercial purposes. Some commenters have suggested that there should be an emphasis on ascertaining the identity of a requester.

Restrictions on scope have been sought by several commenters for interests such as public safety, law and order, sovereign function, privacy of other individuals, legal contraventions and cost. Other commenters have opined that data principals should not be refused access to data on the basis of grounds such as disproportionate effort, costs, volume of data, technical feasibility, inadequate manpower, frivolous claim, and alternate remedy. This is because it will enable data fiduciaries to refuse requests with ease, reduce individual control over data and de-legitimise the idea of a right. The imposition of a reasonable fee for exercise of these rights, as suggested in the White Paper, was widely supported. The exact fee, it was opined, could be determined by delegated legislation or sector-specific regulations. Some commenters were also against levying a fee, as it may discourage data principals from exercising their rights. Here the emphasis is on ensuring that there are no barriers to access data. It was suggested that a cost can be imposed only when requests are vexatious, frequent, unreasonable, or relate to older data.

A few commenters, however have expressed scepticism towards such rights *per se* as they believe that the Indian citizenry lacks awareness of these rights and due to the prospect of unwieldy implementation. However, most commenters supported the recognition of these rights as a necessary tool for the creation of a free and fair data protection framework.

II. Analysis

The right to confirmation refers to the right of a data principal to inquire regarding processing of her personal data by a data fiduciary. The right to access refers to the right of the data principal to gain access to her personal data which is stored with the data fiduciary. This right enables a data principal to gain access to a copy of all the personal data held about him/her by an entity.²²⁶ The basis of these rights is to ensure that the data principal can understand, gauge and verify the lawfulness of processing.²²⁷

The rights to confirmation and access enable a data principal to enforce the substantive obligations of data fiduciaries. Only when a data principal knows what personal data a fiduciary has about herself and how it has been used, can she enforce her rights against the fiduciary. It is important to note that without the right to confirmation and access, the substantive obligations may become mere platitudes. Thus, in principle the rights to confirmation and access must find place in the law.

²²⁶ Ian Long, *Data Protection: The New Rules* (Jordan Publishing, 2016) at p. 25.

²²⁷ Recital 63, EU GDPR.

The scope of these rights must be guided by their rationale. These rights, as evident from the previous paragraph, are gateway rights that allow a data principal to understand the scope and extent of personal data that a fiduciary has. Consequently, these rights allow the data principal to take action, in case there is a breach of a substantive obligation by the fiduciary and are tools which a data principal can use to gauge the lawfulness of data handling by the data fiduciary. Keeping this in mind, the scope of the right to access and confirmation should be broad, and must include:

- (i) All personal data relating to the data principal that has been collected by the data fiduciary;
- (ii) The purposes for which the data fiduciary has collected such data;
- (iii) The entities or persons to whom such data has been disclosed;
- (iv) Information regarding cross-border transfer of such data;
- (v) Information regarding the estimated duration for which data is stored, if feasible; and
- (vi) Such other information regarding the collection, storage, handling and sharing of personal data that would have been provided under the obligation of notice that may need to be accessed again for transparent disclosure to the data principal.

It is to be recognised that the implementation of such an expansive right may be expensive.²²⁸

Further, there may be technical difficulties in complying with requests where large quantities of data are stored in an unstructured manner. After carefully analysing the opinion of commenters, the Committee is of the view that the expense involved in implementing such rights does not provide a principled reason to not have the right in the first place. It does however point to the need to take steps to ensure that these rights are made available by data fiduciaries. To do this, the Committee is of the opinion that a reasonable fee²²⁹ may be charged by the data fiduciary for implementing the right to confirmation and access. Such fee, however, cannot be charged for purposes flowing from point (i) above, which relate to the personal data held by a data fiduciary and its purposes, which must be provided free to the data principal on request.

The DPA may be empowered to set time periods for complying with an access request. The RTI Act, which is akin to an access right only against public authorities, mandates a response in 30 days in the law.²³⁰ However, it is our view that specifying a rigid deadline in a statute as a proxy for reasonableness, without a careful delineation of distinct types of data fiduciaries, the ease or onerousness of the obligations on them and the different types of personal data to

²²⁸Impact Assessment of Proposal for an EU Data Protection Regulation, Ministry of Justice (UK) (2012) available at <<https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/eu-data-protection-reg-impact-assessment.pdf>> (last accessed on 19 April 2018) at p. 18.

²²⁹ Supreme Court Rules, 2013, Third Schedule available at <<http://www.supremecourtofindia.nic.in/sites/default/files/Supreme%20Court%20Rules,%202013.pdf>> (last accessed on 11 May 2018) at p. 63.

²³⁰ Section 7(1), RTI Act.

which access may be sought, may not be advisable. Thus, time periods must be set by delegated legislation. In case it is not feasible to comply within the time period that is set, the data fiduciary will be permitted an additional period to comply.

Data fiduciaries cannot refuse access to data principals on the basis of grounds such as disproportionate effort, costs, volume of data, technical feasibility, inadequate manpower, frivolous claims or any other alternate remedy. The only grounds for such refusal can be any relevant exemptions contained in this law, or any other law, or any other general conditions of refusal for any data principal right (such as, inadequate information regarding the identity of the data principal in the request for the right). Any other grounds for refusal would de-legitimise the idea of a right itself.

Further, the right to rectification (as mentioned in the White Paper) is being referred to as a right to correction in this report, where a data principal shall have the right to correct, complete or update any inaccurate or incomplete personal data about her. It empowers data principals to ensure accuracy of their personal data and may be a natural consequence of the right to access personal data, where such personal data is accessed and found to be inaccurate. The application of this right has a broad scope covering information about the data principal that a fiduciary possesses. It applies to both input personal data and output personal data. Input personal data refers to the data that the data principal provides to the data fiduciary whereas output personal data refers to the data that has been used to create a profile or reach a certain conclusion about an individual.²³¹

It is important to maintain correct and up-to-date personal data in order to ensure the veracity of output decisions. This right is a necessary corollary to implementing the obligation to maintain accurate personal data, which is an obligation on data principals (during input) and data fiduciaries (thereafter). For example, if a data fiduciary analyses the social media activities of a data principal (such as the pages she likes, the videos she watches) and concludes that she likes a particular football club, the data principal will have the right to rectify this conclusion if it is incorrect.

The Committee is of the opinion that data fiduciaries should not be permitted to charge any fee for the implementation of the right to correction as it is the responsibility of the data fiduciary to ensure accuracy of personal data, when it holds such data. A reasonable period, specified by the DPA shall be given to fiduciaries to reflect the corrected data in their systems.

B. Rights to Objection, Restriction and Portability

²³¹ Article 29 Data Protection Working Party, Guidelines on Automated Individual decision-making and profiling for the purposes of regulation 2016/679 (adopted on 6 February 2018) at p. 24.

I. White Paper and Public Comments

The White Paper had some reservations in providing the right to object to processing since the right is only available when the data has been processed on the ground of public interest and legitimate interest (as under the EU GDPR), which may not be included as lawful grounds of processing in our framework.²³² However, the more specific right of objecting to processing for direct marketing was sought to be included within the data protection law, separate from the sector-specific regulations concerning direct marketing.²³³

On the right to not be subject to solely automated decisions, it was of the view that automated decisions may have adverse consequences, and to regulate them a practically enforceable right may be carved out.²³⁴ The White Paper did not hold any provisional views on the right to restrict processing.

Finally, the White Paper concluded that data portability should be included as a right so as to empower data principals to give them control over their personal data. Therefore, the White Paper argued that individuals should be able to access and transfer the data that they have provided in a machine-readable format. Further, the provisional view taken was that all such data should be held in an interoperable format.²³⁵

A significant number of commenters have supported data principal rights, and corresponding provisional views discussed in this chapter. On the issue of the right to object, there was a mixed response. While some commenters agreed with the provisional view that the right to object would not be applicable in the Indian context, some others stated that it is an important right of data principals, which allows them to comprehend the uses of their personal data fully. Most responses however restricted their support of the right to object to that against direct marketing and against solely automated decisions. With regard to the right to object to processing for the purpose of direct marketing, a number of commenters have suggested a strictly consent based approach to direct marketing. Some of them have recommended an opt-out approach, and clear communication to data principals regarding their rights related to direct marketing (at the first stage of communication).

Additionally, a majority of commenters have cautioned against a blanket prohibition on automated decision making. Further, some commenters have stated that the right may only be

²³² White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 18 April 2018) at p. 135.

²³³ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 18 April 2018) at p. 135.

²³⁴ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 18 April 2018) at p. 135.

²³⁵ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 18 April 2018) at p. 135.

applicable when the decision-making is purely through automated means, and the decisions can have potentially harmful or significant legal or economic effects (such as credit, housing, or employment opportunities) on the data principal. There is not much consensus on the applicability of this right where decision-making may have certain elements of human intervention. Some commenters have also generally highlighted the ambiguities and weaknesses of the right in the EU GDPR model.

While a number of commenters have supported a right to restrict processing, they have suggested variations or gradations in the application of this right. For instance, some commenters have advised that the right may only be applicable where personal data is inaccurate, where processing is being done for a commercial purpose, where there is some dispute regarding the legitimate grounds of processing, where the processing is unlawful and so on. On the other hand, some commenters have also argued against the incorporation of a right to restrict processing.

A majority of commenters have supported a right to data portability. However, a significant number of commenters cautioned against the heavy compliance burden on industry, as well as potential roadblocks in implementation. For example, processing a large number of requests for data portability may increase costs for the data fiduciary. In this scenario, a small fee could be charged from the data principal making such a request. Further, some commenters have suggested that it is imperative that data be stored in a standardised or universal machine-readable format. A few commenters have advised that standards related to data portability be developed by the industry.

II. Analysis

These rights represent a particular approach to ensuring lawfulness of processing — by vesting data principals with the power to hold the data fiduciary accountable. It is an extension of the core principle of autonomy, which this report commends as a key plinth of securing a free and fair digital nation. However as discussed previously in the report, autonomy is not absolute and may require to be curbed; not necessarily in favour of competing interests, but rather in the interest of more efficacious achievement of the ultimate public good of a free and fair digital economy. Implicit in such a framework is the need to not only be fair in principle, but fair in practice. This implies the use of the most efficacious method to ensure that processing is lawful and for the purposes for which consent was provided. Such method, may not always rest with the individual.

Keeping this in mind, the treatment of rights in this group can be divided into three sub-categories. First, the rights to object to processing, object to direct marketing and restriction of processing do not fit within the framework of lawful processing established by our framework. Regarding the right to object, in the EU GDPR such rights can be enforced by an individual owing to her particular situation, where the personal data is being processed lawfully under the grounds of public interest, exercise of official authority and legitimate interest. These grounds are not reflected in our framework in the same form as is envisaged

under the EU GDPR. Further, it may be difficult to provide for the specific grounds that would render such an objection valid. It is vague to provide a right to stop lawful processing on the basis of unenumerated grounds.

Finally, to the extent that processing is pursuant to a law or is in furtherance of a non-consensual ground of processing, the onus of protecting the data will have shifted to the law which allows processing in each of these cases. For example, if Aadhaar data can be processed as per the Aadhaar Act by the Unique Identification Authority of India in order to maintain the integrity of the Central Identities Data Repository, processing must be as per the legal provision.²³⁶ If individual circumstances change, then the individual will have a remedy if such change in circumstances renders future processing unlawful. Creating an overriding personal interest, without delineating it, appears ill-conceived.

Regarding the right to object to direct marketing, the Committee has come to the conclusion that data fiduciaries may only engage in direct marketing based on consent of the data principal, which is freely given as per the reinforced standards of our framework. Therefore, if the data principal does not consent to a request to be solicited by direct marketing, a data fiduciary may not be allowed to approach the data principal with marketing material on any mode of communication. This would do away with the need to have a separate right to object to direct marketing. It may be noted that while the TRAI captures a bulk of direct marketing activities that involve calls (via phones or mobiles) and text messages, direct marketing through emails or social media goes unchecked.²³⁷ Therefore, addressing direct marketing through a consent-based framework would optimally fill this void and leave enough room for regulatory action in each sector.

Finally, the right to restrict processing may be unnecessary in India given that it is, in essence, a right given for availing of interim remedies against issues such as inaccuracy of data. Data principals can always approach the DPA or courts for a stay on processing in such cases, and the added benefit of exercising this right directly against a data fiduciary is not clear. Needless to say, the non-existence of this right, will not, in any way, derogate from the data principal's ability to withdraw consent for processing thereby rendering further processing unlawful.

The second group of rights relate to the right to object to automated decision-making and to access the logic behind it. In our view, these rights, again a response by the EU to emerging challenges from Big Data and AI, have a legitimate rationale. They are aimed at curbing harms due to prejudice and discrimination in output data owing to evaluative determinations without human review. The solution provided by this right is to simply involve a step of human review, which is not *per se* immune from prejudice. This is a change pertaining to the operational structure of an organisation. Such a change may be necessitated, provided it is carefully tailored to specific organisations and the nature of their processing activity. This, in

²³⁶ Sections 23(2)(j) and 23(2)(l), Aadhaar Act.

²³⁷ TRAI Telecom Commercial Communications Customer Preference Regulations, 2010, as amended, prohibit unsolicited commercial communications in the form of SMS and calls.

our view, is better achieved through an accountability framework which requires certain data fiduciaries, which may be making evaluative decisions through automated means, to set up processes that weed out discrimination. This is a constituent element of privacy by design which should be implemented by entities proactively, audited periodically and monitored by the DPA in case there are examples of unlawful processing. At the same time, such a model does not entirely denude the individual of agency. If discrimination has ensued as a result of *per se* lawful, yet discriminatory automated processing, individuals are always at liberty to go to courts for breach of fiduciary duties. Thus, the interests underlying such rights, can be more efficaciously achieved by an *ex ante* accountability model.

Third, the right to data portability is critical in making the digital economy seamless. This right allows data principals to obtain and transfer their personal data stored with a data fiduciary for the data principal's own uses, in a structured, commonly used and machine-readable format. Thereby, it empowers data principals by giving them greater control over their personal data. Further, the free flow of data is facilitated easing transfer from one data fiduciary to another. This in turn improves competition between fiduciaries who are engaged in the same industry and therefore, has potential to increase consumer welfare.²³⁸ As the right extends to receiving personal data generated in the course of provision of services or the use of goods as well as profiles created on the data principal, it is possible that access to such information could reveal trade secrets of the data fiduciary. To the extent that it is possible to provide such data or profiles without revealing the relevant secrets, the right must still be guaranteed. However, if it is impossible to provide certain information without revealing the secrets, the request may be denied. The right to transfer or transmit data from one fiduciary to the other should however be limited by constraints of technical feasibility. That is, data fiduciaries would not be obligated to provide data portability if they are able to prove that technical capabilities as currently existing would make the required access or transfer unfeasible.²³⁹ The market standards of technical feasibility of transference of data may be set through codes of practice developed by the DPA to ensure that fiduciaries do not use this reasoning to deny data principals the right to portability. Further, to address concerns of costs, fiduciaries may be allowed to charge a reasonable fee to effectuate this right. In our view, such a balance captures the principled significance of the right while remaining cognisant of the practical difficulties in its implementation today.

C. The Right to be Forgotten

The right to be forgotten refers to the ability of individuals to limit, de-link, delete, or correct the disclosure of personal information on the internet that is misleading, embarrassing, irrelevant, or anachronistic.²⁴⁰ Such disclosure, may or may not be a consequence of unlawful processing by the data fiduciary. This is because, the right flows from the general obligation

²³⁸ Paul de Hert et al., The right to data portability in the GDPR: Towards user-centric interoperability of digital services, *Computer Law & Security Review* (2017) at p. 9.

²³⁹ Article 29 Data Protection Working Party Guidelines on the Right to Data Portability available at <http://ec.europa.eu/newsroom/document.cfm?doc_id=44099> (last accessed on 20 April 2018).

²⁴⁰ Michael J. Kelly and David Satola, The Right to be Forgotten, *University of Illinois Law Review* (2017) at p. 1.

of data fiduciaries to not only process lawfully, but also in a manner that is fair and reasonable. In this context, it is essential to take into account a data principal's understanding of unfairness. Therefore, if she believes certain processing to have unfairly disclosed personal data, then she should be able to have a remedy against such disclosure. The right to be forgotten therefore provides a data principal the right against the disclosure of her data when the processing of her personal data has become unlawful or unwanted.²⁴¹

Implicit in this formulation is the fact that the right itself is defeasible. There is no principled reason as to why the data principal's assessment of unfairness would override that of the fiduciary. Where a disclosure has taken place on the basis of the consent of a data principal, it would be appropriate that the unilateral withdrawal of such consent could trigger the right to be forgotten. In other cases where there is a conflict of assessment as to whether the purpose of the disclosure has been served or whether it is no longer necessary, a balancing test that the interest in discontinuing the disclosure outweighs the interest in continuing with it, must be carried out.

In carrying out this balancing test, certain principled and practical issues must be considered: first, in case of a direct or subsequent public disclosure of personal data, the spread of information may become very difficult to prevent;²⁴² second, the restriction of disclosure immediately affects the right to free speech and expression. The purpose for a publication may often involve matters of public interest and whether the publication is 'necessary' may depend on the extent of such public interest. The appropriateness of a right to be forgotten in these circumstances would require that the right to privacy be balanced with the freedom of speech.²⁴³

I. White Paper and Public Comments

In the White Paper, it was tentatively proposed that the right to be forgotten should be incorporated in the data protection law.²⁴⁴ However, this right must be granted after a careful balancing of the right to freedom of speech and expression with the right to privacy. The

²⁴¹ House of Commons, Justice Committee, *The Committee's opinion on the European Union Data Protection framework proposals: Volume I*, HC 572, (1 November 2012) at p. 26, quoting a former Deputy Information Commissioner of the UK as saying, in relation with an earlier draft of the EU GDPR: "When you unpick it, much of what is there of the right to be forgotten is just a restatement of existing provisions—data shan't be kept for longer than is necessary; if it has been processed in breach of the legal requirements it should be deleted, which goes without saying."

²⁴² House of Lords, European Union Committee, *EU Data Protection law: a 'right to be forgotten'? HL 40* (30 July 2014), the Committee criticised the Google Spain judgment, finding that "Once information is lawfully in the public domain it is impossible to compel its removal, and very little can be done to prevent it spreading. ... A judgment which cannot be complied with brings the law into disrepute."

²⁴³ Thus, in *Lindqvist v Åklagarkammaren i Jönköping*, Case C-101/01, the Court of Justice of the EU found that restrictions on the publication of personal data would require national courts and national legislatures to balance the same against rights such as the freedom of expression. Other considerations may also be relevant. Some Indian courts have grounded this right in the concept of reputation and morality, rather than privacy. In *Vasunathan v. The Registrar General*, High Court of Karnataka, 2017 SCC Karnataka 424, the Court held that while the certified copy of the order may contain the name of the petitioner's daughter, internet search engines will not be permitted to index in sensitive cases involving women in general as it may cause loss of reputation in society.

²⁴⁴ The Supreme Court had also adverted to such a right. Per *Puttaswamy*, (2017) 10 SCALE 1, at p. 33.

White Paper was of the preliminary view that the data fiduciary should carry out this balancing test on the basis of clear parameters.²⁴⁵

There was a division of opinion in public responses on this issue. Some commenters were of the opinion that the right to be forgotten should not be incorporated into India's data protection framework as there is no additional benefit to be gained by guaranteeing this right to individuals. Further, it was argued that incorporating a right to be forgotten would have a detrimental impact on individuals' ability to access information on the internet. Therefore, there is an obvious conflict between balancing this right and other rights such as that of free speech. Alternatively, some commenters believed that the right to be forgotten should be incorporated into India's data protection framework. On the scope of the right, commenters were of the opinion that it should not include the right to erase 'public information' about an individual. Some commenters also agreed that any 'derivatives' of personal data, or data which has been processed by an organisations' algorithms should not be within the scope of this right. Other commenters also argued that certain types of information, such as credit information, criminal history, court orders and so on, should not be permitted to be deleted as they are required in greater public interest, or in interest of law enforcement, or for the purpose of monitoring illegal or fraudulent activities.

On the issue of which entity should carry out the balancing test, some commenters believed that relying on data fiduciaries to make this decision will be excessively burdensome; there is a chance that they will act in their own interest and there will be considerable divergence in practice. Therefore, these commenters suggested that the data protection law should contain specific guidelines, which can be used by data fiduciaries to make their decisions.

II. Analysis

The right to be forgotten is an idea that attempts to instil the limitations of memory into an otherwise limitless digital sphere. A limited memory and the consequent need to both remember and forget are essential facets of the human condition. The internet, with its currently vast reserves of data storage appears to facilitate timeless memory. As a result, the ability to forget is seriously denuded. This might not be entirely undesirable— collective attempts at forgetting have often involved attempts at rewriting history.²⁴⁶

However, the individual desire to forget is an expression of autonomy that may be worthy of protection. This is especially the case, if we accept that data flows are initiated by the individual who must be free and to whom others must be fair. But in considering such a right, it is imperative to note that other individual freedoms and collective goods may be impacted. Removing publicly available information takes away from an individual's right to know; at

²⁴⁵ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 18 April 2018) at p. 141.

²⁴⁶ Howard Zinn, *A People's History of the United States* (Harper Perennial Modern Classics, 2015). For almost two centuries people were told that Columbus was a great hero whereas Howard Zinn's research illuminated how Columbus may actually have been guilty of genocide, torture, rape, enslavement, and thievery.

the same time, it abridges the freedom of the press which has published the story in the first place. Further, if every individual started exercising a right to be forgotten over various types of personal data, the nature of the public realm of information itself would be brought into question as such information may be permanently deleted. Of particular concern is the risk that the deletion may be not just from the public space but also from private storage, preventing later publication as well. Therefore, in order to address these free speech concerns, there may be a need to make a distinction between restrictions on disclosure (such as de-linking in search results) and permanent erasure from storage, which may not be permitted as a separate individual participation right. Further, any implementation of this limited right to be forgotten must involve a careful consideration of the following principled and practical issues:

(a) Balancing the Right with Competing Rights and Interests

The first issue that arises is that the core of the right to be forgotten, i.e. deletion of disclosed or published information, interferes with someone else's right to free speech and expression as well as their right to receive information.²⁴⁷ Further, a broad based right to be forgotten may be susceptible to misuse.²⁴⁸ As discussed above, the Committee is of the view that permanent deletion of personal data from storage should not be a part of this right. While determining whether to allow for the right to be forgotten, the appropriateness of consequent restrictions on the right of free speech and expression and the right to information would necessarily have to be considered.²⁴⁹ This should, however, be constrained through the insertion of a statutory balancing test. Such balance may be achieved through the application of a test with five criteria:²⁵⁰

- (i) the sensitivity of the personal data sought to be restricted.
- (ii) the scale of disclosure or degree of accessibility sought to be restricted.²⁵¹
- (iii) the role of the data principal in public life (whether the data principal is publicly recognisable or whether they serve in public office).
- (iv) the relevance of the personal data to the public (whether the passage of time or change in circumstances has modified such relevance for the public).

²⁴⁷ This has been raised as a matter of considerable concern, with one scholar even referring to the right as ‘the biggest threat to free speech on the Internet in the coming decade.’ See, Jeffrey Rosen, *The Right to Be Forgotten*, 64 Stanford Law Review Online (2012) at p.88.

²⁴⁸ Muge Faz, *Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet*, 3 International Data Privacy Law 3 (August 2013) available at <https://academic.oup.com/idpl/article/3/3/149/622037> (last accessed on 2 June 2018).

²⁴⁹ Mr X v. Hospital Z, 1998 (8) SCC 296. In this case, there was a conflict between the right to privacy of one person and the right to a healthy life of another person. The Court held that, in such situations, the right that would advance public interest would take precedence.

²⁵⁰ These criteria constitute a slight modification of the criteria developed in Google’s internal policy. See, Luciano Floridi et al, Report of the Advisory Council to Google on the Right to Be Forgotten (February 2015) p. 7-14 available at <https://static.googleusercontent.com/media/archive.google.com/en//advisorycouncil/advisement/advisory-report.pdf> (last accessed on 1 May 2018).

²⁵¹ Significantly, in Lindqvist v Åklagarkammaren i Jönköping, Case C-101/01, it was found that the exemption for “personal or household activity” would not apply if the information is “made available to an indefinite number of persons.” The criterion suggested views this question of availability as a question of degree.

- (v) the nature of the disclosure and the activities of the data fiduciary (whether the fiduciary is a credible source or whether the disclosure is a matter of public record; further, the right should focus on restricting accessibility and not content creation).

Since we live in a dynamic digital age, there may be certain situations wherein the information in question (against which a right to be forgotten order was passed) has subsequently become relevant to the public again. Therefore, the law may need to have provisions for the review of such decisions.²⁵²

(b) Appropriate Entity for the Approval of Requests

Considering that the right to be forgotten hinges on the aforementioned balancing test, it is critical to assign this test to an appropriate entity. In the EU, following the recognition of the right to be forgotten, companies like Google received large volumes of requests from individuals for de-listing. EU law envisages that the data fiduciary would have to consider the requests and apply the balancing test mentioned above. In effect, this amounts to the privatisation of regulation and shifts responsibility for the protection of fundamental rights to private entities that are not constrained by democratic accountability. Given that a rejection of de-listing could involve legal consequences for the fiduciary, there may also be considerable incentive to not reject requests, especially when they are in high volume and when the controller does not have the resources to regularly carry out legal assessments. This position of the law in the EU has been criticised on this ground.²⁵³

Further, ‘notice and takedown’ procedures in India (for defamatory and obscene content, for instance) has been seen to be problematic as they appeared to require intermediaries to become private censors determining free speech rights.²⁵⁴ Further, the Supreme Court held in 2015 that under the IT Act, intermediaries should only be required to take down content where they have been notified of objectionable content by the government or through a court order.²⁵⁵

Balancing the right to privacy and other individual interests with the freedom of speech and expression is a core public function. The Supreme Court of India, when faced with a question of competing rights, has laid down a well-established test on how to adjudicate such a question on its merits.²⁵⁶ In India, this balancing function is most appropriately seen as an

²⁵² Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet*, The Centre for Internet and Society (2011) available at <<https://cis-india.org/internet-governance/intermediary-liability-in-india.pdf>> (last accessed on 20 April 2018). It suggests a ‘put-back’ procedure in the context of takedown under the IT Act.

²⁵³ Michael J Kelly and David Satola, *The Right to be Forgotten*, University of Illinois Law Review (2017) at p. 16.

²⁵⁴ Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet*, The Centre for Internet & Society (2011) available at <<https://cis-india.org/internet-governance/intermediary-liability-in-india.pdf>> (last accessed on 20 April 2018).

²⁵⁵ Shreya Singhal v. Union of India, (2015) 5 SCC 1 at para 122.

²⁵⁶ Mr. X v. Hospital Z, 1998 (8) SCC 296.

adjudicatory one. Thus, right to be forgotten requests, in keeping with the scheme of our framework, should be made to the Adjudication Wing of the DPA (as discussed further in Chapter 9).

(c) Breadth of Application of Orders

When a determination has been reached as to the fiduciary's obligation to delete the disclosure of personal data, it becomes essential to ascertain what the breadth of the order is. Where data has been made public, there is every possibility that it has been replicated and published further on other webpages. The EU GDPR provides that a data fiduciary (controller in its language) who has been obliged to delete the disclosure of data should inform other fiduciaries of the data principals' request for deletion. Given that the Committee envisages the right to be one that is granted by the Adjudication Wing of the DPA, whether to impose such obligation or not may be left to the discretion of the relevant Adjudicating Officer and its statutory mandate of narrowly tailoring the exercise of the right. It may be inappropriate to automatically apply orders to other fiduciaries not specifically named in the data principal's request because the approval of a request may have been made on the basis of the nature of the named fiduciary.

RECOMMENDATIONS

- The right to confirmation, access and correction should be included in the data protection law. **[Sections 24 and 25 of the Bill]**
- The right to data portability, subject to limited exceptions, should be included in the law. **[Section 26 of the Bill]**
- The right to object to processing; right to object to direct marketing, right to object to decisions based on solely automated processing, and the right to restrict processing need not be provided in the law for the reasons set out in the report.
- The right to be forgotten may be adopted, with the Adjudication Wing of the DPA determining its applicability on the basis of the five-point criteria as follows:
 - (i) the sensitivity of the personal data sought to be restricted;
 - (ii) the scale of disclosure or degree of accessibility sought to be restricted;
 - (iii) the role of the data principal in public life (whether the data principal is publicly recognisable or whether they serve in public office);
 - (iv) the relevance of the personal data to the public (whether the passage of time or change in circumstances has modified such relevance for the public); and
 - (v) the nature of the disclosure and the activities of the data fiduciary (whether the fiduciary is a credible source or whether the disclosure is a matter of public record; further, the right should focus on restricting accessibility and not content creation). **[Section 27 of the Bill]**
- The right to be forgotten shall not be available when the Adjudication Wing of the DPA determines upon conducting the balancing test that the interest of the data principal in limiting the disclosure of her personal data does not override the right to freedom of speech and expression as well as the right to information of any other citizen. **[Section 27 of the Bill]**
- Time-period for implementing such rights by a data fiduciary, as applicable, shall be specified by the DPA. **[Section 28 of the Bill]**

CHAPTER 6: TRANSFER OF PERSONAL DATA OUTSIDE INDIA

The last two decades have seen an explosive expansion of the internet and the number of internet users across countries. However, what is more significant is that the private nature of internet service providers and the free flow of their services has resulted in the globalisation of the internet as well,²⁵⁷ such that information produced in one country is easily accessible in another. The flow of data remains an imperative for a healthy digital economy. However, a data protection regime that assures individuals of certain rights must ensure that such data flows are not indiscriminate, and that a reasonable level of protection is accorded to such data irrespective of where it is transferred to.

Apart from the legal conditions permitting the flow of personal data across borders, an increasingly relevant method for making jurisdiction effective is to place requirements relating to the storage and processing of personal data within the territory of a state. A policy of storage and processing of personal data within the territorial jurisdiction of a country is advocated to ensure effective enforcement and to secure the critical interests of the nation state. However, due to the substantial costs involved in setting up digital infrastructure to store data locally and in the interests of a free digital economy, the ramifications of such a policy need to be carefully considered. This chapter discusses cross-border flows of personal data as well as requirements for the storage and processing of such data within the territorial reach of a country, outlining the approach of the Committee on these points.

A. White Paper and Public Comments

On the question of when personal data may be transferred abroad, the White Paper identified two preconditions of adequacy and comparable level of protection for such data.²⁵⁸ The provisional view taken was that the adequacy test, which requires the DPA to determine whether a country possessed adequate level of protection for personal data, was beneficial since it ensured a smooth two-way flow of personal data critical for a digital economy.²⁵⁹ In the absence of such a certification, the data fiduciary would bear the responsibility of ensuring that personal data, once transferred would continue to enjoy the same level of protection as in India.²⁶⁰

A majority of commenters suggested that the adequacy test, that requires the DPA to determine if data protection laws in the transferee jurisdiction are adequate (utilised by the EU GDPR in regulating the cross-border flow of data), may be adopted. Interoperability,

²⁵⁷ Orin S. Kerr, The Fourth Amendment and the Global Internet, 67 Stanford Law Review (2015).

²⁵⁸ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 68.

²⁵⁹ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 68.

²⁶⁰ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 68.

greater leverage to access markets and effective protection of citizens' data were key rationales. On the other hand, commenters who argued against the adequacy test reasoned that the determinations were an expensive, time consuming and restrictive process since most countries in the world were yet to adopt laws on data protection. Instead, the principle of accountability was suggested which makes the transferor entity responsible for data protection, where the data crosses borders.²⁶¹

With respect to data localisation, the White Paper recognised the need for treating different types of personal data differently and a one-size-fits-all model was not considered appropriate.²⁶² It was felt that India would have to carefully balance possible enforcement benefits of localisation with the costs involved in mandating such a policy in law.

Commenters were largely unanimous in rejecting a homogenous framework and stressed on the need for sector specific measures along with discretion for a case-by-case determination. However, a majority of the commenters, including major technology companies and industry groups took a view against mandatory data localisation on the basis that such a move may have an adverse impact on the industry. Some commenters supported mandatory localisation of personal data for reasons of law enforcement, preventing foreign surveillance, creating local jobs, ensuring jurisdiction of Indian authorities over data breaches and strengthening of the Indian economy.

B. Analysis

I. Cross-Border Transfer of Personal Data

It is essential to ensure that the interests of effective enforcement of the law, economic benefits to Indians need to be core to any proposed framework for cross-border transfer. However these must not unjustifiably impede international flow of personal data, which itself is beneficial in many ways for Indians. This is similar to the physical economy in India where a combination of free movement of goods and transfer restrictions operate alongside each other. The key questions are where and how the line can be drawn in determining which data can be transferred across borders.

One might wonder why the aforementioned formulation inverts what is perceived to be the status quo, where freedom to transfer is the rule and restrictions on such freedom are the exception. It is only partially accurate to describe the status quo as such. In its operation, the freedom to share personal data in the digital economy operates selectively in the interest of certain countries that have been early movers. For example, the US can, without any detriment to its national interest, support a completely open digital economy by virtue of its technological advancement. The need for local enforcement is also largely accounted for

²⁶¹ Comments in response to the White Paper submitted by Cody Ankeny on 30 January 2018, available on file with the Committee.

²⁶² White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 75.

owing to the personal jurisdiction that the US exercises over a large number of technology companies as well as the large volumes of data stored in its territory.²⁶³ Thus, any advocacy of complete freedom of transfer of personal data in the digital economy, must perhaps be viewed cautiously.

On the other hand, in the EU, the operation of prescriptive rules restricts the permissibility of cross-border transfers to a limited set of circumstances. These include transfers to jurisdictions where data protection norms are deemed ‘adequate’, transfers that are subject to approved contractual clauses or rules, or other prescribed circumstances where the need for transfer is seen to be substantial or the risk of harm is reduced.²⁶⁴ Only 12 countries have received adequacy certification from the EU,²⁶⁵ with data sharing with the US being limited to the privacy shield framework.²⁶⁶ Bilateral agreements have been entered into with the US, Australia and Canada for sharing of airline passenger data for law enforcement.²⁶⁷ Most data sharing to countries other than those that have been deemed ‘adequate’ therefore appears to happen at the level of companies who enter into contracts with standard clauses or through binding corporate rules.

The European Commission has so far issued two sets of standard contractual clauses, first for transfers from data controllers to other data controllers and second for transfer to processors, outside the EU/EEA.²⁶⁸ The contractual clauses, however, have been criticised for not being implementable due to the difficulty faced by DPAs in identifying non-compliance.²⁶⁹ Further, the very validity of standard contractual clauses has been referred to the Court of Justice of the EU, thereby making the future of such transfers uncertain.²⁷⁰ The binding corporate rules

²⁶³ A 2013 report by McKinsey estimated that the US is home to one-third of the world’s data. This translated to 898 exabytes of data (1 exabyte = 1 billion gigabytes). See Game changers: Five opportunities for US growth and renewal, McKinsey Global Institute (July 2013) available at <<https://www.mckinsey.com/featured-insights/americas/us-game-changers>> (last accessed on 23 April 2018).

²⁶⁴ See Chapter 5, EU GDPR.

²⁶⁵ These include Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay. See Adequacy of the protection of personal data in non-EU countries available at <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en> (last accessed on 21 April 2018).

²⁶⁶ The EU-US privacy shield decision was adopted on 12 July 2016 and the privacy shield framework became operational on 1 August 2016. The framework protects the fundamental rights in case of data transfer from the EU to the US for commercial purposes. See EU-US Privacy Shield available at <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en> (last accessed on 21 April 2018).

²⁶⁷ Transfer of air passenger name record data and terrorist finance tracking programme available at <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/transfer-air-passenger-name-record-data-and-terrorist-finance-tracking-programme_en> (last accessed on 21 April 2018).

²⁶⁸ See Model contracts for the transfer of personal data to third countries available at <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en> (last accessed on 21 April 2018).

²⁶⁹ See A. Zinser, The European Commission Decision on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries: an Effective Solution?, 3(1) Chicago-Kent Journal of Intellectual Property, (2003).

²⁷⁰ Clyde & Co, Irish High Court refers validity of model contract clauses to ECJ, Lexology (31 October 2017) available at <<https://www.lexology.com/library/detail.aspx?g=ce3c1970-4382-40df-8de0-3e99ff571d27>> (last accessed on 21 April 2018). The first referral order in The Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (2016 No. 4809 P.) available at

on the other hand only provide a framework for the transfer of data within multinational companies, with the rules requiring approval not only from the DPA appointed as the lead authority for this purpose but also from the DPAs of other EU countries from where the data is being transferred outside the EU.²⁷¹

The discussion above must inform the alternatives that we may consider regarding the permissibility of cross-border transfers of personal data but to understand where we must draw the line, it is imperative to keep in mind India's interests in regulating such transfers. The starting point in this context must be an assessment of the types of personal data to which the law applies. This is the universal set of personal data to which rules relating to cross-border transfers can be applied since (for reasons explained in Chapter 2 on jurisdiction) India's territorial and passive personality interests are impacted. As this is the scope of the law itself, any cross-border flow of other types of data would not be barred by this law. Needless to say, distinct concerns may regulate such activity and the Government may frame a suitable policy in this regard, but such analysis is beyond the remit of our Committee.

Personal data that is maintained in India will always have the protection of India's data protection regime. However, national interest would require that at least an adequate level of protection should be accorded to personal data transferred abroad. Given the mobility and seamless transferability of data, a failure to impose such a restriction would seriously compromise the efficacy of the substantive protections the law provides. It is thus necessary that rules ensuring such adequate protection be implemented.

The question that next arises is how such protection is to be effectuated. It follows from our discussion of the limited nature of adequacy determinations in the EU framework that any analogous model primarily based on such determinations should be looked at cautiously. Though it has significant merits in terms of providing certainty to entities desirous of transferring data, making it the primary method of transfer puts undue enforcement burden on regulators. Whether the DPA in India will have the capacity to do this is an open question, though for a new entity possessing such capacity on Day One is unlikely. Rather, the alternative mode of approved contractual clauses or rules must be improved upon, especially by ensuring that they are in a form that provides adequate protection and are better capable of being enforced.

<<https://www.dataprotection.ie/docimages/documents/Judgement3Oct17.pdf>> (last accessed on 24 April 2018). It is noteworthy to point that in the course of the ongoing Schrems litigation with respect to standard contractual clauses, the Irish High Court has issued a second referral order to the Court of Justice of the EU which questions the validity of the entire EU-US privacy shield itself. See Privacy Shield now facing questions via legal challenge to Facebook data flows (13 April 2018) available at <<https://techcrunch.com/2018/04/13/privacy-shield-now-facing-questions-via-legal-challenge-to-facebook-data-flows/>> (last accessed on 21 April 2018); The second referral order in the case of The Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (2016 No. 4809 P.) available at <<https://www.documentcloud.org/documents/4436535-Ref.html>> (last accessed on 21 April 2018).

²⁷¹ Under the mutual recognition procedure to which 21 EU countries are part of, once the lead authority has concluded that the rules meet all requirements as per law, the other authorities treat the lead authorities' opinion as sufficient basis to issue their own national permits. See Binding Corporate Rules available at <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en> (last accessed on 21 April 2018).

It is our view that the interest of a free and fair digital economy will best be served by a framework where a model contract for such transfers is formulated by the DPA. Entities transferring data would be mandated to incorporate such model clauses in the relevant contracts.²⁷² The model contract will contain the key obligations on transferee entities as per the Indian law. These include security, purpose limitation, storage limitation and a responsibility to fulfil rights of individuals. Further, the transferor entity who is bound by the Indian law will undertake to bear liability for any breach by the transferee in relation to the aforementioned obligations. A self-certification by such entity that the contract is in line with the model contract, and that it undertakes to bear liability as mentioned above, will be recorded. These records will be subject to compulsory audit and periodic reporting to the DPA. A similar set of binding corporate rules which may be termed as ‘intra-group schemes’ can be adopted by group companies for *inter se* transfer of data within the group.

Such entity-led transfers should be the primary method for ensuring equivalent protection for Indian personal data abroad. However, despite the practical difficulties of entering into adequacy assessments, the role of the sovereign in green-lighting certain countries for permissibility of transfer cannot be entirely discounted. This is because, if the very rationale of this law is to protect data of Indians, such rationale will be defeated if data can be transferred abroad without the possibility of any regulatory preconditions being set. The option must be given to the Government of India, in consultation with the DPA to enter such determinations of countries where personal data can be transferred freely. By continuing this option, the law provides a lever for adequacy assessments, contingent on capacity developing over time, reducing transaction costs for entities. However, the law is not contingent on a positive adequacy determination for transfer thereby leaving entities the autonomy to transfer data on the basis of standard contracts. In our view, this is a harmonious balance.

In addition, we may mention that transfers of personal data on the basis of consent have to be permitted. Despite the difficulties this might raise in terms of enforcement, provision for such transfer may be necessary to respect the autonomy of the data principal. For the purposes of sensitive personal data, the consent would have to be explicit (as discussed in Chapter 3). There would however be another exemption to the operation of the regime for the transfer of personal data outside India. There may be a set of hitherto unknown situations where data that is processed must necessarily be transferred abroad without restriction. This may be for practical reasons, e.g. emergencies or strategic ones, or the need to bolster bilateral trade. Since this is best assessed by the executive, the Central Government should have the power to determine such instances on a case by case basis and exempt it from any restrictions (described below) which may apply.

²⁷² For group companies, *inter se* transfers should be permitted based on a standard template that will be pre-approved by the DPA. There will be no need for regular reporting to the DPA every time a contract is entered into or a transfer is made.

II. Exceptions to Free Transfer of Personal Data Outside India

Conditions regarding the permissibility of cross-border transfer of personal data would certainly ensure that data is not deprived of all protection abroad, but it is not enough in and of itself. Despite the conditions discussed above, the imperative of cross-border flow of personal data may have to be balanced with India's interests in enforcing its data protection law in a successful manner. Effective enforcement will invariably require data to be locally stored within the territory of India and this would mean that such a requirement, where applicable, would limit the permissibility of cross-border transfers as outlined above. Different jurisdictions have followed varying practices in this regard. Whereas China localises internet-based mapping services, critical information infrastructure and banking data,²⁷³ Canada localises public interest data held by government agencies, schools and hospitals,²⁷⁴ Australia localises health data²⁷⁵ and so on. In certain cases, such as in jurisdictions like China and Russia, the data that is localised is not permitted to be transferred outside territorial borders.²⁷⁶ In other countries such as Vietnam, a copy of the data is kept on a local server, but data transfer outside the jurisdiction is also permitted.²⁷⁷

Though there is no exact alignment on the categories of data subject to such rules, the rationale is clear: any personal information deemed critical in national interest or for heightened privacy protection is localised. Such rules go beyond the regulation of transfer and take steps towards curtailing flow more strictly. The range of strict restrictions described above appear to be towards one end of the spectrum of barriers that may be placed on the free flow of personal data; this may be compared with the position in the US where there are minimal restrictions as has been discussed in the preceding section of this Chapter.

For the purposes of India, it is the Committee's belief that neither of the above extremes need be the appropriate path. Any obligation requiring the storage and processing of personal data within India should be based on clear advantages arising out of the implementation of such a measure. A policy preventing copies of personal data from being transferred abroad could take two forms: first, a mere requirement to maintain one live, serving copy of personal data (while allowing other copies to be transferred), or second, a stricter requirement that personal data be processed only within India. Both these policies would align with several interests for India, including effective enforcement of the Indian law, promotion of growth in the Indian

²⁷³ Article 31, Cyber Security Law of China provides a non-exhaustive list of selected critical industries and areas whose information infrastructure would be regarded as 'critical information infrastructure'. It includes public communications, information services, energy, transport, water conservancy, finance, public services, and e-governance etc., and more broadly, other information infrastructure, which may cause serious consequences if it suffers any damage, loss of function, or leakage of data. An unofficial English translation of this legislation is available at: The National People's Congress of the People's Republic of China, People's Republic of China Network Security Law (2016) available at <http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm> (last accessed on 8 April 2018).

²⁷⁴ Asia Pacific Economic Cooperation, Cross Border Privacy Rules System. There are currently five participant countries, namely US, Mexico, Japan, Canada and the Republic of Korea.

²⁷⁵ Section 77, Personally Controlled Electronic Health Records Act, 2012.

²⁷⁶ See Article 16(4)(7), Federal Law No. 242-FZ (Russia); Article 37, Cyber Security Law of China.

²⁷⁷ Decree on the management, provision and use of Internet services and online information (No. 72/2013/NĐCP) (Vietnam).

digital ecosystem and avoidance of vulnerabilities in our fibre optic cable network system. Such benefits have been listed in detail below.

(a) Benefits

(i) Enforcement

The question of local storage of personal data is intrinsically connected to the enforcement of domestic law generally and in particular, the data protection law itself. Intelligence agencies and law enforcement bodies have an increasingly challenging role in the 21st century. They must check the growth of terrorism, prevent cyber-attacks and tackle cyber-crime. Investigation of ordinary crime too often requires access to personal data. Further, the obligations on data fiduciaries pursuant to the data protection framework themselves require effective enforcement by the DPA.

In order to fulfil this mandate, law enforcement bodies often need to gain access to information that is held and controlled by data fiduciaries.²⁷⁸ As a result of this, it is important for the law to acknowledge the importance of quick and easy access to information to effectively secure national security and public safety. A requirement to store personal data locally would boost law enforcement efforts to access information required for the detection of crime as well as in gathering evidence for prosecution. This is because it is easier for law enforcement agencies to access information within their jurisdiction as compared to awaiting responses to requests made to foreign entities which store data abroad. However, it is advisable that in the future, nation states should strive towards harmonisation to create an enforcement regime that provides for effective information sharing.

In academic writing, reservations have been expressed against this argument.²⁷⁹ Three claims are made in this regard: first, domestic enforcement may not be hampered by non-availability of data since many laws require cloud service providers to share access with law enforcement agencies; second, business may be driven away because processing data locally would be costly; third, the law may not be followed because controllers ('fiduciaries' in our understanding) would know that the law will be difficult to enforce. It is necessary to consider these arguments carefully.

First, while there may be some degree of compliance with laws having extra-territorial operation, in practice, the enforcement of any order actually made under such laws may be both difficult and time-consuming.²⁸⁰ For non-complying entities outside a particular

²⁷⁸ Tatevik Sargsyan, Data Localisation and the Role of Infrastructure for Surveillance, Privacy, and Security, 10 International Journal of Communication (2016).

²⁷⁹ Anupam Chander and Uyên P. Lê , Data Nationalism, 64 Emory Law Journal (2015).

²⁸⁰ For instance, it has been pointed out that exercising jurisdiction under a law is only one part of the exercise and an authority's intervention could be "rendered futile if its orders against defendants outside its jurisdiction cannot be enforced", see Justice S. Muralidhar, Jurisdictional issues in Cyberspace, 6 The Indian Journal of Law and Technology (2010) at p. 33.

jurisdiction, the enforcing country would be required to issue an MLAT request²⁸¹ to the country enjoying personal jurisdiction over the entity. The MLAT process is well documented to be deeply flawed and overly time-consuming and therefore recourse to such a regime may not be the ideal enforcement solution unless adequate improvements are effected in the future.²⁸²

Second, any argument highlighting the costs arising from the domestic retention of personal data must meet a higher burden. All or most legal obligations give rise to economic costs for regulated entities and thus mere increase in costs cannot be reason not to introduce legal change. Rather, it must be shown that the costs incurred due to rules demanding local processing outweigh the benefits of such a requirement. This must be done while keeping in mind that the benefits run to the core objectives of data protection. While some commenters have suggested that mandating storage and processing locally may have significant financial implications, the real question is whether the actual costs of local processing will be such that it overrides the benefits of companies having access to the burgeoning consumer database in India.²⁸³ There is no evidence presented before us that demonstrates the results of this cost-benefit analysis conclusively.

Third, that the law will not be enforced is not an adequate justification. For instance, while the enforcement status of similar laws in Russia and China are unclear, the enforceability of any such rules would depend on local enforcement capacity and prioritisation. This argument puts the cart before the horse.

It is important to note that currently, eight of the top 10 most accessed websites by individuals in India are owned by US entities.²⁸⁴ Therefore, there is a high probability that, in order to conduct an investigation, enforcement bodies may have to request some of these US entities for information. Although, we do not have a record of the number of requests that have been sent to these companies by enforcement agencies in India, we found that the UK government had sought customer data for at least 53,947 separate user accounts controlled by American technology companies in the year 2014.²⁸⁵ Further, between January and June 2017, Google received 3,843 user data disclosure requests by Indian governmental agencies

²⁸¹ Shalini S., Evaluating MLATs in the Era of Online Criminal Conduct, CCG Working Paper Series No. 2 (2015-16).

²⁸² For some practical suggestions to make the MLAT regime effective, see Bedavyasa Mohanty and Madhulika Sri Kumar, Hitting Refresh: Making India-US Data Sharing Work, Observer Research Foundation Special Report No. 39 (2017) available at <<https://www.orfonline.org/wp-content/uploads/2017/08/MLAT-Book.pdf>> (last accessed on 7 June 2018).

²⁸³ According to Indiastat.com, India has an estimated population of 1,344,283,227 at present. The projected population for 2050 is 1,807,878,574, Estimated Population, Indiastat available at <<https://www.indiastat.com/popclockflash.aspx>> (last accessed on 8 April 2018).

²⁸⁴ Alexa, Top Sites in India available at <<https://www.alexa.com/topsites/countries/IN>> (last accessed on 21 March 2018).

²⁸⁵ Andrew Keane Woods, Against Data Exceptionalism, 68 Stanford Law Review (2016) at p. 743.

of which in 54% of the cases some data was produced.²⁸⁶ Thus, Google refused to provide data in 46% of the cases.

It is not our claim that with a mandate to process data locally, perfect compliance will be achieved, and all requests will be automatically answered (or even, should be answered). This is because despite the data being located physically in India, a conflict of law question might arise if the country of the concerned entity's registration or any other country with which the entity or the claim is substantially connected, also asserts jurisdiction.²⁸⁷

However, if personal data that is within the remit of the data protection law is processed in India (in this case, personal data of persons present in India, collected by an entity outside India offering services to persons present in India or carrying on business in India), then the possibility of a foreign entity refusing access to such data would be reduced. Further, even if such access were denied, the fact of the physical location of the data being in India would be a key factor in a conflicts determination of which court will have jurisdiction over the matter. Thus, a requirement to store or process personal data locally would certainly aid domestic enforcement significantly and this can be achieved by requiring that at least one copy of the personal data be maintained within the territory of India.

(ii) Avoiding resultant vulnerabilities of relying on fibre optic cable network

A large amount of data is transmitted from one country to the other via undersea cables. For instance, Tata Communications owns and operates the world's largest subsea cable network which reaches a large number of countries representing 99.7 per cent of the world's GDP.²⁸⁸ There have been studies which show that undersea cable networks are significantly vulnerable to attack.²⁸⁹ A report by Policy Exchange highlights that sabotage of undersea cable infrastructure is an existential threat to the UK. The result would be to damage commerce and disrupt government-to-government communications, potentially leading to

²⁸⁶ Google Transparency Report, Overview: India available at <https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts;authority:IN&lu=legal_process_breakdown&legal_process_breakdown> (last accessed on 8 April 2018).

²⁸⁷ In this context, the case of United States v. Microsoft, 584 US _ (2018) was argued in the US Supreme Court in February 2018. Law enforcement in the US claimed jurisdiction over personal data in relation to a crime in the US. The data itself was stored on a server in the Republic of Ireland. A jurisdictional question arose. For case history, see United States v. Microsoft Corporation, Oyez available at <<https://www.oyez.org/cases/2017/17-2>> (last accessed on 9 May 2018). If there were a localisation mandate to store such data in the US, the case would have been rendered moot. As it happens, the question has become superfluous by the passage of the CLOUD Act by the US Congress.

²⁸⁸ Tata Communications completes world's first wholly owned cable network ring around the world, Press Release - Tata Communications (22 March 2012) available at <<https://www.tatacommunications.com/press-release/tata-communications-completes-worlds-first-wholly-owned-cable-network-ring-around-world/>> (last accessed on 29 January 2018).

²⁸⁹ Ryan Singel, Fibre optic cable cuts isolate millions from the Internet, Wired (31 January 2008) available at <<https://www.wired.com/2008/01/fiber-optic-cab/>> (last accessed on 29 January 2017); Alexandra Chang, Why undersea Internet cables are more vulnerable than you think, Wired (4 February 2013) available at <<https://www.wired.com/2013/04/how-vulnerable-are-undersea-internet-cables/>> (last accessed on 29 January 2017).

economic turmoil and civil disorder.²⁹⁰ Further, the location of almost every undersea cable in the world is publicly available,²⁹¹ which increases the risk of vulnerability of the internet and cross-border transfer of data.²⁹²

From this, it may be argued that data critical to Indian national interest should be processed in India as this will minimise the vulnerability of relying solely on undersea cables. Critical data, in this context will include all kinds of data necessary for the wheels of the economy and the nation-state to keep turning. It is thus a wider category than the determination of data in respect of which foreign surveillance needs to be prevented and may include health, government services, infrastructure data and system control software which includes *inter alia* transport, waterways and all controlled and sensor mapped infrastructure. This may even extend beyond the scope of personal data, regarding which an appropriate call may have to be taken by the Government of India. The objective will be served if even a single live, serving copy of such critical personal data is stored in India. However, the processing of such data exclusively within India may be necessary for other benefits as discussed below.

(iii) Building an AI ecosystem

In the coming years AI is expected to become pervasive in all aspects of life that are currently affected by technology and is touted to be a major driver of economic growth.²⁹³ For instance, a study by the consulting company Accenture has estimated that AI has the potential of adding 1.6 percentage points to China's economic growth by 2035 owing to China's recognition of the importance of AI and its commitment to investments in its development.²⁹⁴ India's addition is expected to be USD 957 billion by 2035 (1.3 percentage points to be added to GDP).²⁹⁵ Therefore, the economic potential of an AI ecosystem is immense.²⁹⁶ Developments in this direction are thus integral to creating a thriving digital economy.

²⁹⁰ Rishi Sunak, Undersea cables: Indispensable, Insecure, Policy Exchange (2017) available at <<https://policyexchange.org.uk/publication/undersea-cables-indispensable-insecure/>> (last accessed on 29 January 2017).

²⁹¹ Submarine Cable Map, Telegeography (2017) available at <<https://www2.telegeography.com/submarine-cable-map>> (last accessed on 29 January 2018).

²⁹² It may be noted that mandating the storage of all personal data locally could raise its own security concerns as the centralisation of all such data in one location would potentially make it more vulnerable, see for example, Anupam Chander and Uyên P. Lê , Data Nationalism, 64 Emory Law Journal (2015) at pp. 715-720. However, these concerns are of reduced significance because, as is discussed below, only a smaller sub-set of all personal data can be made subject to a mandate of local storage in India.

²⁹³ Shripati Acharya, The great Indian data rush, Yourstory (26 February 2018) available at <<https://yourstory.com/2018/02/great-indian-data-rush/>> (last accessed on 23 April 2018).

²⁹⁴ How Artificial Intelligence can drive China's Growth, Accenture (2018) available at <<https://www.accenture.com/cn-en/insight-artificial-intelligence-china>> (last accessed on 23 April 2018). For a more detailed analysis of the impact of AI on China's economic growth, see Artificial Intelligence: Implications for China, McKinsey Global Institute (April 2017) available at <<https://www.mckinsey.com/~media/McKinsey/Global%20Themes/China/Artificial%20intelligence%20Implications%20for%20China/MGI-Artificial-intelligence-implications-for-China.ashx>> (last accessed on 23 April 2018).

²⁹⁵ Rewire for Growth: Accelerating India's Economic Growth with Artificial Intelligence, Accenture (2017) available at <https://www.accenture.com/t20171220T030619Z_w_in-en_acnmedia/PDF-68/Accenture-ReWire-For-Growth-POV-19-12-Final.pdf%20-%20zoom=50> (last accessed on 21 April 2018).

The growth of AI is heavily dependent on harnessing data, which underscores the relevance of policies that would ensure the processing of data within the country using local infrastructure built for that purpose. This is because currently most of the personal data of Indian citizens, such as the data collected by internet giants such as Facebook and Google are largely stored abroad.²⁹⁷ Azmeh and Foster²⁹⁸ in their 2016 study, point out the benefits that developing countries can derive from a policy of data localisation. These include: first, higher foreign direct investment in digital infrastructure and second, the positive impact of server localisation on creation of digital infrastructure and digital industry through enhanced connectivity and presence of skilled professionals. Creation of digital industry and digital infrastructure are essential for developments in AI and other emerging technologies, therefore highlighting the significance of a policy of requiring either data to be exclusively processed or stored in India. This benefit can be captured in a limited manner by ensuring that at least one copy of personal data is stored in India. Further, a requirement to process critical data only in India would create a greater benefit insofar as it extends beyond mere storage.

(iv) Preventing foreign surveillance

Finally, one of India's key interests with regard to personal data which is critical to India's national security interests and imperative for the smooth running of the wheels of the Indian economy is the prevention of foreign surveillance. It has been argued by some scholars that requirements of storing data within territorial borders may be useful in boosting data security by safeguarding the privacy and security of personal information against non-governmental actors.²⁹⁹ Largely, major information intermediaries such as Facebook, Google, Amazon, Uber, etc. are headquartered in the US. Consequently, a significant portion of the data collected by some of these entities are stored in the US³⁰⁰ and in other countries around the world thereby increasing the scope of foreign surveillance. Based on such access to the data or presence in a foreign jurisdiction, laws of foreign countries may potentially allow

²⁹⁶ In fact, the Ministry of Commerce and Industry, Government of India has recognized the importance of AI and constituted a Task Force on Artificial Intelligence which has submitted a report on the subject, see Report of the Artificial Intelligence Taskforce available at <http://dipp.nic.in/sites/default/files/Report_of_Task_Force_on_ArtificialIntelligence_20March2018_2.pdf> (last accessed on 7 June 2018).

²⁹⁷ Shripathi Acharya, The great Indian data rush, Yourstory (26 February 2018) available at <<https://yourstory.com/2018/02/great-indian-data-rush/>> (last accessed on 23 April 2018).

²⁹⁸ Shamel Azmeh and Christopher Foster, The TIPP and the digital trade agenda: Digital industry policy and Silicon Valley's influence on new trade agreements, London School of Economics Working Paper No. 16-175, (2016) at pp. 26-27 available at <<http://www.lse.ac.uk/international-development/Assets/Documents/PDFs/Working-Papers/WP175.pdf>> (last accessed on 23 April 2018).

²⁹⁹ See Jack Goldsmith, Unilateral Regulation of the Internet: A modest defence, 11(1) European Journal of International Law (2000); Alexander Savelyev, Russia's new personal data localization regulations: A step forward or a self-imposed sanction?, Computer Law and Security Review 32 (2016); John Selby, Data Localisation laws: trade barriers or legitimate responses to cybersecurity risks, or both?, 25(3) International Journal of Law and Information Technology (2017).

³⁰⁰ Google Data Centres, Google available at <<https://www.google.com/about/datacenters/inside/locations/index.html>> (last accessed on 7 February 2018); Facebook Data Centres, available at <<http://www.datacenterknowledge.com/data-center-faqs/facebook-data-center-faq>> (last accessed on 7 February 2018).

surveillance. This is not fear-mongering — the PATRIOT Act amendments to FISA have precisely this effect.³⁰¹

If data is exclusively processed in India, it will potentially cut off foreign surveillance of large amounts of such data. It is essential to recognise that the logical consequence of accepting this rationale is to advocate the processing of data only in India. Doing so for all kinds of data will create an Indian internet that will be walled away from the rest of the internet. Such a measure is clearly overbroad and hurts the prospect of a free and fair digital economy. Furthermore, it is not narrowly tailored to the type of data, surveillance of which is considered particularly detrimental. This would be precisely the kind of policy that ought to be avoided being based on ideological, as opposed to strategic, principled or practical considerations.

In order to strike a balance, it is essential to enquire into the kinds of surveillance activities that are most detrimental to national interest. In the context of personal data, this would pertain to such critical data as those relating to Aadhaar number, genetic data, biometric data, health data, etc. Only such data relating to critical state interests must be drawn up for exclusive processing in India and any such obligations should be limited to it. All other kinds of data should remain freely transferable (subject to the conditions for cross-border transfer mentioned above) in recognition of the fact that any potential fear of foreign surveillance is overridden by the need for access to information. Thus, for prevention of foreign surveillance critical personal data should be exclusively processed within the territory of India.

However, despite these advantages of partial or complete restrictions on cross-border flow of data, it is also important to consider the various costs that may be associated with the implementation of such a policy.

(b) Costs

(i) Economic and Market Implications

³⁰¹ Federal Bureau of Investigation, Testimony available at <<https://archives.fbi.gov/archives/news/testimony/usa-patriot-act-amendments-to-foreign-intelligence-surveillance-actAuthorities>> (last accessed on 8 April 2018) “Section 207 of the USA PATRIOT Act changed the law as to permit the government to conduct electronic surveillance and physical search of certain agents of foreign powers and non-resident alien members of international groups for initial periods of 120 days, with extensions for periods of up to one year...section 214 of the USA PATRIOT Act simplified the standard that the government must meet in order to obtain pen/trap data in national security cases... Section 215 of the USA PATRIOT Act allows the FBI to obtain an order from the FISA Court requesting production of any tangible thing, such as business records, if the items are relevant to an ongoing authorized national security investigation, which, in the case of a United States person, cannot be based solely upon activities protected by the First Amendment to the Constitution”; see also, Sections 218 and 504 of the PATRIOT Act; Snowden disclosures helped reduce use of PATRIOT Act provision to acquire email records, The Guardian (29 September 2016) available at <<https://www.theguardian.com/us-news/2016/sep/29/edward-snowden-disclosures-patriot-act-fisa-court>> (last visited on 8 April 2018). Edward Snowden’s disclosures have had the effect of curtailing the expansion of these provisions.

Any requirement to store and process data locally may impose a substantial economic burden on domestic enterprises that provide goods and services with the help of foreign infrastructure such as cloud computing.³⁰² One way of viewing this problem is to consider how the market would respond to such a mandate. Large foreign companies may be willing and able to invest in new servers within the territory where they want to operate. However, the costs of creating or renting such newly built infrastructure may be high for a number of small and medium-sized businesses (including domestic ones) that would otherwise have been able to afford cheaper foreign cloud service providers. By raising such entry barriers, such a mandate may thus aggravate existing issues like the monopolisation of the digital economy and monopolisation of data by foreign companies that have already been enjoying first-mover and network industry advantages in the last few decades. Allowing international flow of services would likely reduce the costs of data processing by small Indian companies looking to enter into the digital economy.

As discussed above, the representations made to us have not persuaded us of the possible economic implications of local storage and processing of personal data in India. It is our considered view that the size and potential of the Indian market trumps the additional cost that some entities may have to bear on account of a mandate to process personal data locally. Further, for small players, options of storing data on local clouds will only increase pursuant to our recommendation. Finally, by not making the requirement of processing of personal data in India absolute (applying to all kinds of data) and restricted to critical personal data (no transfer of data abroad), any onerous effects on smaller entities will be significantly obviated.

(ii) Balkanisation of the Internet and Domestic Surveillance and Censorship

Apart from the abovementioned considerations of data as a question of international trade and economic activity, the flow of personal data is specifically linked with the rights to free speech and privacy.

The availability of information about one nation in others has meant that the latter nations effectively become checks on the veracity and integrity of information in the former. Thus, if information about law enforcement actions against an individual in Country A is publicised from a website with servers in Country B, the government of Country A cannot compel or influence (including through the threat of force or sanctions) the website into modifying its information at the original copy in the servers.³⁰³ On the contrary, mandating the processing of personal data locally might lead to harassment, censorship or worse still, self-censorship. Thus, some see this as a threat to free speech as all information about a country may become

³⁰² The weighted impact of localisation on the GDP of the EU is estimated to be about 0.4% (See An Economic Assessment of Data Localisation Measures in the EU Member States, European Centre for International Political Economy available at <<http://eipe.org/app/uploads/2016/12/Unleashing-Internal-Data-Flows- in-the-EU.pdf>> (last accessed on 11 May 2018).

³⁰³ See Jonah Hill, The Growth of Data Localisation Post-Snowden: Analysis and Recommendations for US Policymakers and Business Leaders, The Hague Institute for Global Justice, Conference on the Future of Cyber Governance (2014) at p. 28 (finding that the internet has furthered, “individual participation in the political process, increased transparency of governmental activities, and promoted fundamental rights”).

subject to filtering in a manner that was made impossible in the last couple of decades due to the rise of the internet.³⁰⁴ The internet could get splintered into multiple subnets that are subject to more direct and comprehensive control by domestic governments with each being capable of covert control over content and accessibility. Domestic surveillance could also receive a substantial advantage as a result of increased access to the relevant data and the accompanying chilling effects can be greatly enhanced. In short, such a requirement of either requiring the maintenance of local copies of personal data or limiting the processing of personal data to India might derivate from the free and fair digital economy that we would like to create.

While this argument has a certain intuitive appeal, on reflection it suffers from certain logical flaws. First, merely because data is located in a country does not render it vulnerable to censorship. If censorship is indeed made possible, it requires, in addition, a dysfunctional data protection law that allows governments the tools to facilitate such censorship. It is certainly not an automatic consequence of local retention or restriction to local processing.

Second, several kinds of access restrictions take place today, without the requirement of local retention or processing, through blocking orders ('internet shutdowns'). The merits of such shutdowns are a distinct issue; the relevant point in this context is that access restrictions are possible without a mandate to store personal data locally as well.

Finally, the vision of several national internets entirely walled to the outside world is currently a caricatured characterisation that evokes fear of changing the status quo. So was the concept of the nation state bounded by territory and based on the principle of national sovereignty in the 17th century. If the unit in which sovereignty is vested and exercised is the nation state, it is inevitable that a movement towards making the nation state the central actor in internet governance will emerge.³⁰⁵ The desirability of such movement cannot be assessed against the reference point of what the internet is today or was when it began. On the contrary, it requires a holistic assessment of the ongoing geopolitical changes in the world to understand what the internet might become. Thus, acting on a nostalgic understanding of what the internet was like when it started to defer a mandate to store and process personal data locally will be myopic. There is no principled or practical reason to believe that the very fact of local storage or restriction to local processing itself will make the digital economy any less free or fair. On the contrary, it will ensure more effective enforcement of substantive obligations that are directed towards these objectives. It will be free and fair, but possibly different from the internet we have today.

³⁰⁴ Erica Fraser, Data Localisation and the Balkanisation of the Internet, 13(3) SCRIPTed available at <<https://script-ed.org/article/data-localisation-and-the-balkanisation-of-the-internet/>> (last accessed on 14 May 2018); Christopher Kuner, Data Nationalism and Its Discontents, 64 Emory Law Journal (2014) at pp. 2089 and 2097; Anupam Chander & Uyên P. Lê, Data Nationalism, 64 Emory Law Journal (2015) at pp. 677, 680 and 735.

³⁰⁵ This is the basic argument made by Lawrence Lessig who talks of the future of internet regulation as "competition among sovereigns". Lawrence Lessig, *Code: Version 2.0* (Basic Books, 2006) at pp. 306-310.

On the basis of the above discussion, it is the Committee's view that a three-pronged model should be followed. First, all personal data to which the law applies should have at least one live, serving copy stored in India. Second, in respect of certain categories of personal data that are critical to the nation's interests, there should be a mandate to store and process such personal data only in India such that no transfer abroad is permitted. Third, the Central Government should be vested with the power to exempt transfers on the basis of strategic or practical considerations thereby facilitating free flow of data across borders where justified. While these measures may not lead to perfect compliance, it is expected to significantly bolster domestic enforcement and reduce reliance on the MLAT request regime.

The Central Government should determine the categories of personal data for exclusive storage in India not just with regard to enforcement but also strategic interests of the State. Given the strictness of such an obligation, exceptions need to be laid down to allow for cross-border transfers even when exclusive storage is mandated. For instance, in respect of categories such as health data, cross-border transfers will have to be permitted where certain prompt action needs to be taken in order to protect the life or health of an individual. For example, the medical data of an Indian national may be transferred from one hospital in India to a hospital abroad where she is admitted for emergency treatment.

Transfers of critical personal data may also be permitted to those countries which have been green-lighted under the adequacy assessment for the purpose of cross-border transfers of personal data generally (as discussed above). However, the Central Government should only permit such transfers of critical personal data where necessary and provided that it does not hamper enforcement.

This model, in our view, strikes a harmonious balance between the interests of internet users, companies and the nation state in ensuring that data of persons present in India is both protected and used to empower them in their daily lives.

RECOMMENDATIONS

- Cross border data transfers of personal data, other than critical personal data, will be through model contract clauses containing key obligations with the transferor being liable for harms caused to the principal due to any violations committed by the transferee. **[Section 41(1)(a) of the Bill]**
- Intra-group schemes will be applicable for cross-border transfers within group entities. **[Section 41(1)(a) of the Bill]**
- The Central Government may have the option to green-light transfers to certain jurisdictions in consultation with the DPA. **[Section 41(1)(b) of the Bill]**
- Personal data determined to be critical will be subject to the requirement to process only in India (there will be a prohibition against cross border transfer for such data). The Central Government should determine categories of sensitive personal data which are critical to the nation having regard to strategic interests and enforcement. **[Section 40(2) of the Bill]**
- Personal data relating to health will however permitted to be transferred for reasons of prompt action or emergency. Other such personal data may additionally be transferred on the basis of Central Government approval. **[Section 41(3) of the Bill]**
- Other types of personal data (non-critical) will be subject to the requirement to store at least one serving copy in India. **[Section 40(1) of the Bill]**

CHAPTER 7: ALLIED LAWS

A. Impact on Allied Laws

The processing of personal data is omnipresent in the public and private sector. Currently norms relevant to data protection are spread across various statutes, which may lack overall consistency and general applicability. This creates ambiguity and irregularity in the protection of an individual's personal data. The proposed data protection framework must outline the minimum standards that will have to be followed and will have an impact on processing of personal data in all sectors, irrespective of more specific and overlapping sectoral statutes and regulations.

Various allied laws are relevant in the context of data protection because they either require or authorise the processing of personal data for different objectives. Data protection laws usually make room for the legislature to privilege particular objectives for the processing of personal data in specific situations. All such laws, however, will have to be applied along with the data protection law, as the latter will be the minimum threshold of safeguards for all data processing in the country. Similarly, the law will operate in tandem with extant legislation. In the event of any inconsistency, it will have overriding effect. In other words, no other law will operate in derogation of it. However, if a higher standard for protection of personal data is imposed by another law (for instance, the draft Digital Information Security in Health Care Bill, 2017), it may operate in addition to the proposed data protection law.

The Committee has identified a list of 50 statutes and regulations which have a potential overlap with the data protection framework. **Annexure C** is attached to this report, listing such laws that may be affected. Concerned ministries may take note of this and ensure appropriate consultation to make complementary amendments where necessary.

Regardless of the overlapping effect of a data protection regime on other enactments, certain other enactments require to be amended simultaneously with a data protection regime. Three such enactments have been identified for disparate reasons. The Aadhaar Act needs to be amended significantly to bolster privacy protections and ensure autonomy of the UIDAI. Since the context of the Committee's functioning has been shaped by a vigorous public debate about Aadhaar and its impact on data protection, the Committee would be remiss if it did not deal with this issue. Second, the RTI Act prescribes a standard for privacy protection in laying out an exemption to transparency requirements under Section 8(1)(j). This has often been used to deny RTI requests in the past and requires harmonisation with the data protection framework proposed by us. Third, the data protection statute replaces Section 43A of the IT Act and the SPD Rules issued under this provision. Consequently, this provision requires to be repealed together with consequent minor amendments. Since the first two of these amendments require explanation, they are dealt with fully below.

B. Amendments to the Aadhaar Act

Much public attention around data protection issues has centred around Aadhaar and the possibility that creating a database of residents would be antithetical to a well-functioning data protection regime. The validity of arguments regarding its constitutional aspects has been litigated extensively in the Supreme Court in *Puttaswamy*.³⁰⁶ Since the judgment is awaited, no comment is being made on the merits or demerits of such arguments and counter-claims.

However, it is salient that the data protection regime proposed by the Committee will require close introspection by the Government on various aspects pertaining to the existing functioning of the UIDAI. Currently the Aadhaar Act is silent on the powers of the UIDAI to take enforcement action against errant companies in the Aadhaar ecosystem. This includes companies wrongly insisting on Aadhaar numbers, those using Aadhaar numbers for unauthorised purposes and those leaking Aadhaar numbers, all of which have seen several instances in the recent past. Each of these can affect informational privacy and requires urgent redressal.

In addition, recent announcements of the UIDAI relating to the Virtual ID — creating an alias for authentication keeping the Aadhaar number out of the knowledge of the entity requesting authentication — and offline verification — allowing identity verification using QR codes without keeping a centralised record, have significant potential to ensure both collection limitation and data minimisation. However, there is no statutory backing for such announcements as on date and it is unclear as to how they are to be effectively implemented.

Amendments are thus necessary to the Aadhaar Act for bolstering privacy protections for residents as well as reconceptualising the UIDAI into a regulatory role that can ensure consumer protection and enforcement action against violations with appeals to an appropriate judicial forum. It is to be noted that this Committee is neither tasked with nor intends to suggest large-scale amendments to the Aadhaar Act itself. The amendments that are recommended are limited to those warranted by the need to bring the Aadhaar Act in line with the suggested data protection framework. These amendments, when read with several provisions in the draft data protection bill, particularly those in Chapter XI relating to penalties and remedies for aggrieved individuals, ought to alleviate data protection related concerns surrounding Aadhaar.

Accordingly, two broad sets of amendments to the Aadhaar Act are necessary:

First, amendments to bolster the right to privacy of individuals would be required. A critical obligation on all data fiduciaries is collection limitation, i.e. collection of personal data should be limited to such data necessary for processing. Accordingly, amendments have been suggested that classify requesting entities into two kinds to regulate access to personal data

³⁰⁶ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, W.P. (Civil) No. 494/2012 Etc.

on the basis of necessity — those who can request for authentication and those who are limited to verifying the identity of individuals offline.

Regarding entities who can request for authentication, as a matter of principle, the same should be restricted to any entities which perform a public function and require verifiable identification for the purpose of performing such public function. This principle is captured by allowing any entity to request for authentication in two situations: first, if it is mandated by law made by Parliament. The Parliament, as the highest law-making body in the country is within its sovereign power to require individuals to authenticate themselves when it feels necessary. If any entity requests authentication pursuant to a parliamentary mandate, the same must be respected. It is expected that Parliament will be judicious in determining which entities require such authentication. Second, a public authority performing a public function that is approved by the UIDAI may also seek authentication. In granting such approval, the UIDAI should take into account security standards employed by the entity as well as the steps it has taken to incorporate privacy protections for Aadhaar number holders.

Further, the UIDAI may classify such requesting entities that are entitled to seek authentication into those which can directly access the Aadhaar number, i.e. authentication *simpliciter*, and those which can only access the Virtual ID, an alias of the Aadhaar number. The Virtual ID is a temporary 16-digit random number, which can be generated by an Aadhaar number holder for certain types of authentications. It does not reveal the individual's Aadhaar number. This distinction is significant to ensure that only those entities which require the Aadhaar number itself for their functioning, collect the Aadhaar number and other entities only collect the Virtual ID. This is how collection limitation can be upheld in the Aadhaar framework.

For entities which do not perform a public function, identification of individuals may still be necessary. Currently, many such entities, as a matter of course, ask for the Aadhaar number of individuals. This represents a significant privacy concern. For all such entities, only offline verification of Aadhaar numbers with the consent of the Aadhaar number holder may be used to verify the identity of an individual. This mechanism would ensure that sensitive information related to individuals such as their Aadhaar number is not disclosed to requesting entities for routine activities and transactions.

In this entire scheme, in order to ensure that privacy protection goes hand in hand with substantive benefits for individuals, all requesting entities are mandated to ensure that in case there is an authentication failure owing to *bona fide* reasons such as infirmity, disability or technical failure, alternate means of identification (such as offline verification or others) should be made available. This has been made obligatory on all requesting entities. Further, it has been reiterated that core biometric information shall not be shared with anyone as the highest standard of protection is necessary for it.

Second, amendments are required to ensure the autonomy of the UIDAI. With over 121 crore Aadhaar numbers having been issued, the Government of India and State Governments

making Aadhaar authentication mandatory for several benefits, subsidies and services, and several private transactions using Aadhaar as a method of identification, the need of the hour is a regulatory framework for the operation of Aadhaar. This requires two conceptual changes to the way in which the Act currently conceives of the UIDAI— first, the UIDAI must be autonomous in its decision-making, functioning independently of the user agencies in the government and outside it, that make use of Aadhaar; second, the UIDAI must be equipped with powers akin to a traditional regulator for enforcement actions.

After having examined the powers and functions of existing statutory regulators such as TRAI, SEBI, CCI, etc. and the deficiencies in the existing framework for Aadhaar, the Committee is of the considered view that the UIDAI must be vested with the functions of ensuring effective enforcement, better compliance, consumer protection and prevention and redress of privacy breaches. Accordingly, powers should be given to the Authority to impose civil penalties on various entities (including requesting entities, registrars, and authentication agencies) that are errant or non-compliant. In cases involving statutory violations or non-compliance, or an actual or impending privacy breach, the UIDAI will be tasked with the power to issue directions, as well as cease and desist orders to state and private contractors, and other entities discharging functions under the Aadhaar Act.

This will work in tandem with the provisions of the draft data protection bill which will allow all aggrieved individuals to approach the Data Protection Authority in case of violation of the data protection principles, against any entity in the Aadhaar ecosystem, including the UIDAI itself, when it is a data fiduciary. Taken together, this will ensure that aggrieved citizens have appropriate remedies against all entities handling their Aadhaar data and errant entities in the Aadhaar ecosystem are subject to stringent enforcement action.

Finally, to bolster the financial autonomy of the UIDAI as a regulator, amounts received from penalties levied by the Authority under the Act will be deposited in a separate fund. This is critical if UIDAI is to play the role of a responsible regulator and a responsible data fiduciary.

The proposed changes will be instrumental in addressing significant privacy concerns that have been raised relating to the Aadhaar framework. They will also ensure that the UIDAI is more autonomous in its functioning, and has the necessary regulatory tools to protect privacy interests of Aadhaar number holders. Finally, in its role as a data fiduciary under the proposed data protection framework, the UIDAI will, in the eyes of the data protection law, be viewed as any other entity processing personal data of individuals, and will be subject to the rigours and penalties of the law. It is thus critical that these changes be made hand-in-hand with a new data protection legislation.

To make the aforementioned changes, it would be necessary to carry out certain amendments to the Aadhaar Act on the lines of the suggestions made in the Appendix to this Report. The Government may consider such amendments as it may deem appropriate and take suitable legislative measures to implement them.

C. Amendments to the RTI Act

Data protection law is designed to limit the processing of personal data to legitimate reasons where the flow of information is beneficial and respects the autonomy of the data principal. It is particularly sensitive to the harm to an individual pursuant to the disclosure of personal data and seeks to actively prevent such harm.

However, disclosure of information from public authorities may lead to private harms being caused. It is thus important to recognise that, in this context, there is a conflict of fundamental rights, between transparency and privacy. This requires careful balancing. The fact that neither the right to privacy nor the right to information is absolute and will have to be balanced against each other in some circumstances has been recognised by the Supreme Court.³⁰⁷ This balance is sought to be achieved by the exemptions in Chapter II of the RTI Act.

Chapter II of the RTI Act grants citizens a right to obtain information from public authorities and a procedure is put into place for dealing with requests for such information. However, certain exemptions are provided for in Section 8 of the Act in which case the disclosure of the requested information is not necessary.

Of relevance is the exemption in Section 8(1)(j) which reads:

- (1) Notwithstanding anything contained in this Act, there shall be no obligation to give any citizen, --
(j) information which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information.

Provided that the information which cannot be denied to the Parliament or State Legislature shall not be denied to any person.

The section creates a test which balances the right to privacy of a person against the right of a third party to seek information. The section requires the Public Information Officer to generally provide information, unless such information has no relationship to any public activity or interest or causes unwarranted invasion of privacy. These tests may sometimes work against the interests of transparency. To give an illustration, the Supreme Court has

³⁰⁷ *Thalapallam Ser. Coop. Bank Ltd. v. State of Kerala* (2013) 16 SCC 82 (“Right to information and Right to privacy are, therefore, not absolute rights, both the rights, one of which falls under Article 19(1)(a) and the other under Article 21 of the Constitution of India, can obviously be regulated, restricted and curtailed in the larger public interest. ... Citizens' right to get information is statutorily recognized by the RTI Act, but at the same time limitations are also provided in the Act itself ...”)

held that the *performance of an employee/officer in an organisation is primarily a matter between the employee and the employer and normally those aspects are governed by the service rules which fall under the expression “personal information”, the disclosure of which has no relationship to any public activity or public interest.*³⁰⁸ While releasing documents such as Annual Confidential Reports may not be desirable in all circumstances,³⁰⁹ it is questionable whether the performance of a public servant is indeed a matter which has no relationship to any public activity or interest. If the condition that the information bears no relation to any public activity or public interest is met, the burden shifts on the seeker of information to establish that the disclosure of the information is in larger public interest.³¹⁰ This may often be a difficult burden to bear as the citizen may not be in possession of any material to establish any specific concern involving larger public interest. Further, this defeats the spirit of the RTI Act which sees transparency as an end in itself, and not necessarily a means to an end.

The other condition in Section 8 (1)(j) for denial of information, i.e. “which would cause unwarranted invasion of privacy” also raises complex issues. First, there is no indication in the provision as to what constitutes an unwarranted invasion of privacy. This problem may be exacerbated by the enactment of a data protection law which gives a broad definition of personal data. A lot of information sought from a public authority may contain personal data of some kind or another. Further a strict interpretation of purpose limitation may give rise to the inference that any disclosure other than for the purpose for which the personal data was submitted would lead to an unwarranted invasion of privacy. For instance, if a citizen entertains a well-founded suspicion that an unqualified candidate has been appointed to a post by a public authority, she would be well within her right to seek information relating to educational qualifications submitted by the employee as part of the recruitment process. That such personal data was submitted for the purposes of evaluation *alone* should not be a bar to disclosure for being contrary to the purpose limitation provision of the data protection bill.

To avoid this predicament, the RTI Act must specifically spell out the circumstances in which disclosure of such personal information would be a proportionate restriction on privacy having regard to the object of the RTI Act in promoting transparency and accountability in public administration.³¹¹ This must be done keeping in mind the fact that the RTI Act generally leans in favour of disclosure of information.³¹²

The fact that information is in the custody of a public authority gives rise to a presumption that it is information available to a citizen to access. The burden then falls upon the public authority to justify denial of information under one of the exceptions. This is a critical feature of the design of the RTI Act and the Committee finds that this must be preserved notwithstanding a data protection law.

³⁰⁸ *Girish Ramachandra Deshpande v. Central Information Commissioner* (2013) 1 SCC 212.

³⁰⁹ *RK Jain v. Union of India* (2013) 14 SCC 794.

³¹⁰ *Girish Ramachandra Deshpande v. Central Information Commissioner* (2013) 1 SCC 212 para 13.

³¹¹ See long title of the Right to information Act, 2005.

³¹² *Surupsingh Naik v. State of Maharashtra* (2007) 4 Mah LJ 573.

The question then arises as to what are the exceptional circumstances in which personal data can be denied to a citizen. Here, the relevant factor should be any likely harm that may be caused to the data principal by the disclosure of such information. As noted above, the RTI Act, in most circumstances, leans in favour of disclosure, underlining the importance of transparency in public activities. The Committee is cognizant of the fact that this feature of RTI Act has contributed tremendously to securing the freedom of information and enhancing accountability in public administration. This feature has to be accounted for in any balancing test created under the RTI Act. Therefore, in addition to the likelihood of harm, disclosure should be restricted only where any likely harm outweighs the common good of transparency and accountability in the functioning of public authorities.

Accordingly, the proposed amendment to Section 8(1)(j) has three features:

First, nothing contained in the data protection bill will apply to the disclosure under this section. This is to prevent privacy from becoming a stonewalling tactic to hinder transparency.

Second, the default provision is that the information which is sought must be disclosed. It is assumed that such disclosure promotes public interest and the common good of transparency and accountability.

Third, only if such information is likely to cause harm to a data principal and such harm outweighs the aforementioned public interest, can the information be exempted from disclosure.

The Committee finds that such a formulation offers a more precise balancing test in reconciling the two rights and upholding the spirit of the RTI Act without compromising the intent of the data protection bill.

RECOMMENDATIONS

- Various allied laws are relevant in the context of data protection because they either require or authorise the processing of personal data for different objectives.
- All relevant laws will have to be applied along with the data protection law, as the latter will be the minimum threshold of safeguards for all data processing in the country. In the event of any inconsistency between data protection law and extant legislation, the former will have overriding effect.
- The proposed data protection framework replaces Section 43A of the IT Act and the SPD Rules issued under that provision. Consequently, these must be repealed together with consequent minor amendments. **[First Schedule of the Bill]**
- The RTI Act prescribes a standard for privacy protection in laying out an exemption to transparency requirements under Section 8(1)(j). This needs to be amended to clarify when it will be activated and to harmonise the standard of privacy employed with the general data protection statute. **[Second Schedule of the Bill]**
- The Committee has identified a list of 50 statutes and regulations which have a potential overlap with the data protection framework. Concerned ministries may take note of this and ensure appropriate consultation to make complementary amendments where necessary.
- The Aadhaar Act needs to be amended to bolster data protection. Suggested amendments for due consideration are contained in the Appendix to this Report.

CHAPTER 8: NON-CONSENSUAL PROCESSING

Despite the importance of consent in the legal framework, reasons other than consent may, on occasion, be relevant bases for processing of data. This is consistent with our normative framework— while consent, as an expression of autonomy is constitutive of a free and fair digital economy, so are other interests. Thus, it is only a combination of individual autonomy together with such other valuable interests that make a free and fair digital economy possible and it is only in such a normative framework that autonomy and such other interests are meaningfully protected.³¹³

The critical question for determination in the law would be what the circumstances are where consent is either not appropriate, necessary, or relevant for processing. To understand the nature of the interests owing to which non-consensual processing will be permitted, a useful starting point would be the *Puttaswamy* judgment. Chandrachud, J., identified four ‘legitimate state interests’ to be considered in the context of privacy. He listed ‘national security’, ‘prevention and investigation of crime’, ‘protection of revenue’ and ‘allocation of resources for human development’ of which the first three are straightforward state functions that serve collective interests. The fourth which pertains to allocation of resources for human development with the aim of preventing wastage of public resources belongs to a distinct category and is considered under the head ‘functions of the State’.

In addition to the illustrative list of “legitimate state interests” provided by Chandrachud, J., two other interests may be equally weighty—ensuring compliance with law and complying with a judicial order. Further, non-consensual processing may be relevant to the promotion of a free and fair digital economy in matters relating to use of personal data for journalism and purely domestic or personal purposes. While these are not state interests, they are societal interests which are better served by the free flow of information without hindrance. Finally, certain weighty individual interests may also override the consent requirements of this law, such as prompt action to save the life of an individual need not adhere to the terms of consent as per this law. Needless to say, other obligations on data fiduciaries may continue to apply.

It is necessary to note that this chapter deals with two categories of processing that are ordinarily dealt with separately in law: (i) grounds other than consent for processing; and (ii) exemptions from the law.³¹⁴ This conflation is deliberate for the purpose of conceptual clarity — each of these cases, whether processing for national security or prompt action to save the life of an individual, is characterised by the fact that a non-consent based ground for processing is used. However, an important distinction must be drawn between the non-consensual grounds of processing and exemptions. Grounds of processing represent non-consensual bases for processing of personal data that address situations where it is not

³¹³ This is not a utilitarian argument that is sacrificing individual interest for collective interest. Rather it is a Razian argument that all such interests together constitute a notion of the common good. See Joseph Chan, Raz on Liberal Rights and the Common Good, 15(1) Oxford Journal of Legal Studies (1995).

³¹⁴ Such a framework has been followed by the EU GDPR which specifically provides non-consensual grounds of processing and thereafter lays down specific categories of exemptions in the law.

possible to obtain consent or consent may not be an appropriate ground for processing. All other obligations under the law are ordinarily applicable to such processing and any incursion into privacy is minimal. Most exemptions, on the other hand are non-consensual grounds of processing which are exempt from substantive obligations under the law and constitute restrictions on the right to privacy.

Non-Consensual Grounds for Processing

A. White Paper and Public Comments

The White Paper suggested that grounds for processing other than consent should be recognised since it is not always possible to obtain consent in all situations.³¹⁵ Grounds such as performance of contract and necessity for compliance with law were considered to be intuitively necessary.³¹⁶ A suitable adaptation of the “legitimate interest” ground in the EU GDPR was suggested for India.³¹⁷ The White Paper was of the view that there should be a residuary ground under which data could be processed, as it was not possible for a data protection law to foresee all situations which may warrant the processing of personal data without seeking consent.³¹⁸ Commenters overwhelmingly agreed with the need for recognising grounds for processing other than consent. Several commenters were however of the opinion that the law should be prescriptive, and no residuary ground should be retained due to possibility of interpretational ambiguities. One of the alternatives suggested to a “grounds of processing approach” was a two-tiered model based on: (i) legitimate purpose where data could be processed without consent (based on grounds such as legal necessity, to undertake certain risk mitigation activities, to carry out judicial and administrative orders, to carry out processing activities necessary for the prevention and detection of illegal activities and fraud); and (ii) a rights-based framework where once consent had been given, the data fiduciary would ensure that data was being processed in a manner which would not violate the rights of the individual, including the right to be treated fairly and without bias, the right of the individual to seek information relating to the uses to which her personal data would be put or disclosed, and that such data would be processed in accordance with the highest standards of security and safety.³¹⁹

B. Analysis

³¹⁵ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 103.

³¹⁶ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 103.

³¹⁷ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 104.

³¹⁸ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 104.

³¹⁹ Comments in response to the White Paper submitted by Shivakumar Shankar, Managing Director of LexisNexis Risk Solution, 30 January 2018, available on file with the Committee.

Based on a review of academic literature, international best practices and comments received in response to the White Paper, the Committee has identified the following non-consensual grounds for processing which are relevant to the Indian context. The scope and description of these grounds of processing are set out below.

I. Functions of the State

(a) Context

As has been pointed out before, a data protection law, to be meaningful should, in principle, apply to the State. It would indeed be odd if a law enacted to give effect to a fundamental right to privacy does not serve to protect persons from privacy harms caused by processing of personal data by the State.

While for several interactions with the state, consent would be the norm for processing of personal data, the suitability of consent as a ground for processing of personal data by the state performing a state function, raises several questions. Some functions of the state are of a nature that consent may not be an appropriate ground for processing. In several situations, where the State interacts with the citizen, the imbalance of power between them would very often affect the validity of the consent given. The ongoing debate about Aadhaar squarely raises this issue. When a citizen is to receive a welfare benefit, the validity of any consent given is questionable. The problem is exacerbated if the consent is given by a person in dire need of essential services or goods. The interaction between the state and the citizen in this context cannot be compared to that of a consumer entering into a contract with a service provider. The option available to a consumer in refusing an onerous contract and choosing another service provider is not available to a person seeking a welfare benefit from the state.

Similarly, the State also collects large amounts of personal data in the performance of its regulatory functions. For instance, the approval of a building permission by a local body is subject to the submission of an application which is bound to contain personal data of the applicant. Any attempt to obtain consent, particularly where a citizen or person seeks approval from the State is bound to be reduced to a formality. If on the other hand, genuine consent is to be operationalised in these circumstances, collective interests stand to suffer. For instance, from the last example, few would argue that a building permission can be given even if information necessary to evaluate the plan is withheld by the applicant.

There may be other situations where the state may need access to various data sets for performing certain functions. For example, one of the functions of a District Planning Committee, as per various State District Committee Planning Acts, is to prepare a suitable employment plan.³²⁰ In furtherance of this goal, the District Planning Committee may collect

³²⁰ Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679, (2017) at p.7; UK Information Commissioner's Office, When is consent appropriate? available at <https://ico.org.uk/>

personal data of individuals in the district as part of this exercise. If such a function is to be conditional on consent, and such consent is to meet the standard discussed above, it would be open to persons to not participate in the exercise, thus skewing the accuracy of the data set.

Mindful of the functions of the State, various jurisdictions have created non-consensual grounds of processing personal data in exercise of public functions. For example, in the EU the ground of processing of public function of the State applies when a public authority carries out its tasks, duties, functions and powers (including its discretionary powers). These functions are required to be those that have been set out under law.³²¹ Such law need not necessarily be an explicit statutory provision.³²² The ground would be relevant so far as the law's application is clear and foreseeable for the overall purpose for which the public function is to be carried out and a legal basis for each specific activity within such purpose may not be needed.

As per the EU GDPR, the relevant task or function that the public authority is performing should nonetheless have a basis in law. The lawful basis of such a public function should be documented and the official authority acting as data fiduciary should be able to identify a basis, for example in statute or common law for the activity for which they process personal data.³²³ Therefore, a public function of the state can be carried out only if it is in furtherance of such law. Consequently, any processing that is undertaken by the official authority beyond what is envisaged under law would not be permitted under this ground of processing. It is imperative to draw a distinction between 'public function' and 'compliance with law'. While the latter restricts processing to mandatorily comply with the letter of the law, "public function" extends it to performing acts which are in furtherance of the law through a grant of powers or discretion.

If the public authority in question is able to demonstrate that it is exercising its lawful and legitimate authority and that the processing is necessary for such exercise, there is no additional obligation on such authority to prove that the purpose is actually part of a public function. In this instance, the term "necessary" would mean that the processing should be targeted and proportionate to the purpose.

A natural extrapolation of the above principle is that an organisation which is deemed to be a public authority could rely on this ground to carry out processing of personal data but is necessarily limited by its lawful functions. Where activities are excluded from the scope of an authority's legally prescribed public function, the authority would have to rely on consent or some other ground of processing.

[organisations/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/) (last accessed on 13 July 2018).

³²¹ Article 6(3), EU GDPR.

³²² Recital 41, EU GDPR.

³²³ UK Information Commissioner's Office, Public Task available at <<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/>> (last accessed on 7 May 2018).

(b) Scope

In determining the scope of non-consensual processing by the state in India, regard must be had to three factors: the nature of the entity performing the function, the nature of the function and last, the extent to which personal data can be processed. All three factors must be satisfied in accordance with the discussion below for non-consensual processing to apply.

First, only bodies covered under Article 12 of the Constitution may rely on this ground. The established jurisprudence of Article 12, including the meaning of ‘other authorities’ under the Article would create an adequate check on the kinds of bodies that may process personal data.³²⁴ Illustratively, these entities include ministries and departments of the Central and State Governments, bodies created by or under the Constitution, Parliament, and State Legislatures. These entities are assigned specific functions of governance but may also carry out activities that are private in nature. The latter should not be the basis for processing under the ground. Processing towards such activities, including by government companies, will not be permitted under this ground as the second factor to be satisfied, i.e. that it is for the performance of a public function, will not be met.

Second, permitting non-consensual processing by entities above for all kinds of public functions may be too wide an exception to consent (private functions being performed by these bodies are anyway excluded from this ambit). The Supreme Court, in *Puttaswamy*, while commenting on the need for non-consensual processing of personal data by the State observed:

*In a social welfare state, the government embarks upon programmes which provide benefits to impoverished and marginalised sections of society. There is a vital state interest in ensuring that scarce public resources are not dissipated by the diversion of resources to persons who do not qualify as recipients. Allocation of resources for human development is coupled with a legitimate concern that the utilisation of resources should not be siphoned away for extraneous purposes. Data mining with the object of ensuring that resources are properly deployed to legitimate beneficiaries is a valid ground for the state to insist on the collection of authentic data. But, the data which the state has collected has to be utilised for legitimate purposes of the state and ought not to be utilised unauthorisedly for extraneous purposes. This will ensure that the legitimate concerns of the state are duly safeguarded while, at the same time, protecting privacy concerns. Prevention and investigation of crime and protection of the revenue are among the legitimate aims of the state. Digital platforms are a vital tool of ensuring good governance in a social welfare state. Information technology – legitimately deployed is a powerful enabler in the spread of innovation and knowledge.*³²⁵

³²⁴ Ajay Hasia v. Khalid Mujib (1981) 1 SCC 722; Pradeep Kumar Biswas v. Indian Institute of Chemical Biology (2002) 5 SCC 111; Zee Telefilms v. Union of India (2005) 4 SCC 649.

³²⁵ *Puttaswamy*, (2017) 10 SCALE 1 at para 181.

Drawing from the above observation, it is possible to envisage processing of personal data for two particular kinds of functions. First, personal data may be collected to the extent necessary for the provision of any service or subsidies in the nature of welfare benefits. Second, the State should be allowed to collect personal data to the extent necessary for the performance of regulatory functions. Such functions are, undoubtedly, intrinsically linked to ensuring governance. These could include the issuance of licenses, permits or approvals by the Executive. An extensive exercise may need to be carried out for the identification of the various bodies within the Central Government and State Governments that constitute data fiduciaries as well as to demarcate specific functions of such bodies for which this ground can be relied upon. Here, it is important to stress that only those bodies which are performing functions directly connected to such activities should be allowed to use this ground. Further, such functions must be specifically authorised by law. A large part of the functioning of various departments of Government may be indirectly or remotely connected to the promotion of public welfare or regulatory functions. The ground cannot be used to justify the processing of personal data for all such functions. For functions not covered under this ground, the State, like other private actors, must rely on consent as the ground for processing personal data.

Third, while processing personal data under this ground, the state should not collect personal data more than what is necessary for a legitimate purpose. In the case of consent, a data fiduciary can potentially collect personal data even beyond what is strictly necessary for any task, where the data principal consents to such collection. Processing of data by the state on the basis of a non-consensual ground must be strictly confined by necessity. The State should not collect more personal data than what is necessary for any stated purpose and any systematic collection of data is to be preceded by an assessment of the extent to which data collection would be proportionate having regard to the legitimate purpose at hand. This requires to be stressed in the context of the provision of welfare benefits. Processing of personal data should, in no case, take the form of a coercive measure to collect more information than is necessary for any legitimate purpose associated with the provision of such benefit. Any such processing would fail to meet the requirement of fair and reasonable processing under the law.

(c) Application of Obligations

As is clear from the observation in *Puttaswamy*, it is the strict application of data protection obligations which will ensure that the personal data of citizens and other data principals are not misused even where such processing is non-consensual. Thus, even in those situations where the State may insist on the collection of data for certain functions, the state should rigorously abide by data protection obligations. Particular regard should be had to principles such as data minimisation, purpose limitation and transparency. The state should provide clear notice of purpose when it collects data from citizens and processing must be confined to the stated purposes and must be carried out in a transparent manner. Given the higher standards of accountability expected of the state,³²⁶ it is only such fair and reasonable processing that will enable citizens and other data principals to trust the state with their personal data.

II. Compliance with Law or Order of Court or Tribunal

(a) Context

There are certain legal obligations which involve the processing of personal data, either for the fulfilment of a purpose or direction outlined in law or compliance with an order of a court or tribunal. Similarly, personal data that is processed pursuant to a court or tribunal order would be covered. Such collection will be justified under the ground of compliance with a law or order of court or tribunal. It is important to have this ground of processing in order to ensure that the data protection law does not hinder the application of obligations and compliances under other laws and the adjudicatory system. Realising the importance of the same, a number of countries have recognised this ground of processing.³²⁷

This ground will not apply if the collection, use or disclosure of personal data is not mandatory under a valid law or order of a court or tribunal. For example, if personal data is

³²⁶ Even in matters of contract, the State is expected to be fair and cannot act like a private body. *New Horizons Limited v. Union of India*, 1995 (1) SCC 478

³²⁷ Article 6(3), EU GDPR; Recital 41, EU GDPR; Information Commissioner's Office, Legal Obligation available at <<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legal-obligation/>> (last accessed on 5 May 2018); Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller (2014) at p. 19; Sections 11 and 12 POPI Act; Section 1, South African Revenue Service Act, 1997; Section 84 read with Schedule 9 (3) of the UK Data Protection Bill. The EU GDPR permits processing when it is necessary for the compliance with a legal obligation. The legal obligation need not necessarily be an explicit statutory obligation. Therefore, delegated legislation in the form of rules and regulations and common law obligations will also constitute law as long as the application of the law is foreseeable to those data principals subject to it. However, processing of data beyond what is required by law through voluntary unilateral engagements and public-private partnerships will not be permitted. In South Africa, personal information may be processed if processing complies with an obligation imposed by law on the responsible party. Further, personal information need not be collected from the data subject if it is required to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue. The UK Data Protection Bill contains a provision similar to the EU GDPR wherein processing is allowed as long as it is necessary for compliance with a legal obligation to which the controller is subject, other than an obligation imposed by contract.

used or disclosed under a contract, this ground would not be applicable.³²⁸ Further, this ground of processing will only extend to laws passed by Parliament or State Legislatures and subordinate legislation therein, and orders of courts or tribunals in India. It will not cover a duty or obligation of data fiduciaries arising out of a foreign law, treaty or international agreement (unless such duty or obligation is also specifically recognised through domestic law), or orders delivered by foreign courts.

(b) Scope

In our view, a separate ground for compliance with law or order of court or tribunal should be recognised in order to avoid inconsistency with obligations under other laws and judicial orders. The word ‘law’ shall be construed to mean laws, ordinances, orders, bye-law, rules, regulations and notifications as per Article 13 of the Constitution (with the exception of custom and usage). However, processing under any rules, notification or any other delegated legislation must be based on some statutory authority. Obligations imposed by contract and foreign law shall not be permitted to be processed under this ground. An order of court or tribunal would be restricted to Indian courts and tribunals. Processing of sensitive personal data may be permitted only if it has been explicitly mandated under any law made by Parliament or the Legislature of any State or order of a court or tribunal in India.

The Committee notes that there may be some overlap between the ground permitting non-consensual processing in compliance with law and the ground relating to functions of the state discussed above. This ground accommodates processing of personal data which has been made mandatory under any law. This may be undertaken by private actors acting in compliance with a law. For instance, a company is required to file annual returns which may contain personal data of individuals such as promoters, directors or key managerial personnel.³²⁹ It would be superfluous for a taxation authority to seek consent of an assessee before collecting information when such collection has been made mandatory under a law. As with the previous ground, what is critical is the amount of information which can be collected under any such law. Any statute mandating processing of personal data must meet the requirement of proportionality to be constitutional vis-à-vis the right to privacy.

(c) Application of Obligations

It should be noted that if processing is undertaken under this ground, it must comply with the data protection law in general.³³⁰ Obligations such as purpose limitation and collection limitation will apply since personal data may only be collected as sanctioned by the law or judicial order under which the data is being collected and processed. In other words, the data

³²⁸ Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller (2014) at p. 19.

³²⁹ Section 92 of the Companies Act 2013.

³³⁰ More specifically, the requirements of necessity, proportionality and purpose limitation; See Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller (2014) at p. 19.

protection law will supplement all existing laws permitting data collection so as to ensure that any processing of personal data respects the right to informational privacy of citizens. The only exception to this principle will be where a statute has explicitly prescribed higher norms of data protection in which case, such obligations can apply to the exclusion of provisions under this law.

As with the previous ground, the right to data portability may not be suitable since the entity maintaining the personal data is likely to be doing so for a purpose which may not allow for the transfer or deletion of such data. Thus the right to data portability will not apply in these two non-consensual grounds for processing.

III. Prompt Action

(a) Context

There may be cases where an individual's personal data may be processed in an emergency health situation, or when there is a significant risk to the individual's health and safety. In such cases, seeking consent prior to processing may be onerous, or entirely impossible. For instance, rescue operations, transporting a road accident victim to the hospital, contacting the next of kin of a dying person, and large-scale rescue operations during natural disasters would fall under this category. To permit processing in such situations, it is necessary to have a ground for prompt action.

It is important to note that while the application of this ground is limited to particular situations involving questions of life and death of the data principal and threat of injury, it is not necessary for such threat to be immediate.³³¹ Therefore, this ground of processing can be used for collecting, using or sharing data in situations when the harm is not immediate such as when there is a threat of epidemiological disease.³³² Moreover, this ground can be used in situations when there is risk of significant harm to life,³³³ where processing is necessary for humanitarian emergencies (disaster management) and where processing is necessary to protect the data principal's life or health. The importance of this ground is further bolstered by the fact that a number of countries have recognised it.³³⁴

³³¹ Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller (2014) at p. 20.

³³² Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller (2014) at p. 20.

³³³ Data Protection and Sharing- Guidance for Emergency Planners and Responders available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60970/dataprotection.pdf (last accessed on 6 May 2018).

³³⁴ Article 6(d), EU GDPR; Article 9 (2) (c) read with Recital 112, EU GDPR; Section 76 read with Schedule 10 (3), UK Data Protection Bill; Section 11(d), POPI Act. As per the EU GDPR, this ground is permitted to be used where processing is necessary in order to protect the vital interests of the data principal or of any other person. Additionally, in situations where 'processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent', the ground of vital interest may be invoked. The UK Data Protection Bill has a provision similar to the EU GDPR. In South Africa, processing is permitted if it protects the legitimate interest of the data principal. Therefore, while the

(b) Scope

The Committee is of the view that this ground should be extended to the following situations: (i) where there is a threat to life or health of a data principal; (ii) for provision of medical treatment or health services to individuals during an epidemic, outbreak of disease or any other threat to public health; and (iii) for ensuring safety of individuals and to provide assistance or services to individuals during any disaster or during a breakdown of public order. It should only be invoked when it is impractical or impossible to use any other ground for processing. Further, it should be strictly interpreted and must only be applied in critical situations where the individual is incapable of providing consent and the processing is necessary for fulfilling any of the aforementioned situations. Processing of certain categories of sensitive personal data such as sex life, sexual orientation, caste or tribe, or religious or political affiliation or belief, transgender and intersex status however should not be permitted under this ground as they would not be relevant to any measures of prompt action.

(c) Application of Obligations

Notice provisions, as laid out in the data protection law shall not be applicable to processing carried out under this ground, if it substantially prejudices the purpose for such processing. All obligations relating to purpose limitation, collection limitation, storage, accuracy, security safeguards and the data principal rights shall continue to apply since personal data processed in an emergent situation should be limited to the purposes it was processed for and must be securely kept for as long as is necessary and disposed of thereafter.

IV. Employment

(a) Context

There are a large number of situations where an employer may find it necessary to process personal data pertaining to their employees or to their potential employees. For instance, employers may need to collect personal data from individuals for the purpose of recruitment. This may include personal data such as the names, addresses and educational qualifications that a potential candidate might include in her application form. Employers may also find it necessary to process personal data of their employees during the course of their employment relationship, which might include bank account details, PAN card numbers etc. for the purpose of paying their salaries. Other personal data, which an employer may collect and process may include medical records, records pertaining to promotions, disciplinary matters, attendance records and so on. In many situations, processing activities in relation to the above could be carried out on the basis of consent of the individual or even on the ground of

scope of application is wider than the EU model, it is limited to only the data principal whereas the EU GDPR extends vital interest to “any other person” as well.

legal compliance, where the employer is required or authorised by law to collect, disclose³³⁵ or process certain types of personal data.

However, these grounds alone may not be sufficient or appropriate in certain circumstances for the purpose of carrying out processing activities in the context of employment. For instance, the data protection law sets out that for consent to be valid, it must be free, informed, clear, specific and capable of being withdrawn. By this logic, employees are seldom in a position to freely give, refuse or revoke consent due to the nature of the relationship between the employer and the employee and the inherent dependency of the employee on the employer.³³⁶ There may also be several processing activities which require the employer to seek consent from the employee multiple times, or on a regular basis. Seeking consent in this manner may involve a disproportionate effort on the part of the employer or may lead to consent fatigue on the part of the employee.

Further, relying solely on compliance with law as a ground for processing in an employment context is also not adequate as there are many other types of personal data such as collection of attendance records which are not mandated by law.

(b) Scope

The Committee is of the view that this ground should be extended to the following situations: (i) recruitment or termination of employment of a data principal; (ii) provision of any service to or benefit sought by an employee; (iii) verifying the attendance of an employee; or (iv) any other activity relating to the assessment of the performance of the employee. This ground should be invoked only where it involves a disproportionate or unreasonable effort on the part of the employer to obtain valid consent of the data principal, or where validity of the consent is in question due to the unique nature of the relationship between the employer and employee. This ground may be used when the type of processing activity which is required to be undertaken by the employer does not fall within any of the other grounds.

(c) Application of Obligations

All obligations will be applicable on data fiduciaries who are carrying out processing activities in the context of employment. Therefore, the employer must adhere to the principles of collection limitation and purpose limitation and collect only as much personal data as may be required to satisfy their purpose. The employer, as a data fiduciary, must also

³³⁵ Section 45(2)(c), Employees' State Insurance Act, 1948 stipulates that an employer may be required to furnish books, accounts and other documents relating to the employment of persons and payment of wages upon request to the Social Security Officer. Similarly, Section 13(2)(a), Employees' Provident Funds and Miscellaneous Provisions Act, 1952 provides that an Inspector has the power to require an employer to furnish such information as may be necessary.

³³⁶ Article 29 Data Protection Working Party, Opinion 02/2017 on data processing at work at p. 3; Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679, (2017) at p.8; UK Information Commissioner's Office, When is consent appropriate? available at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/> (last accessed on 13 July 2018).

adopt any such organisational measures as may be necessary in order to safeguard the personal data being processed. Other obligations such as storage limitation and accuracy will also apply to the employer.

The employer should give employees sufficient notice detailing the personal data being collected, the purpose for which it is being processed, and the third parties to whom such data may be disclosed and so on. Further, data principal rights of confirmation, access, correction and portability will also be available to the employees.

V. Reasonable Purpose

(a) Context

There is a need for a residuary ground for processing activities which are not covered by other grounds like consent, compliance with law, prompt action and public function but are still useful to society. The primary advantage of having “reasonable purpose” as a ground of processing is the flexibility it affords to data fiduciaries.³³⁷ This ground would be applicable in situations where data fiduciaries may need to carry out processing for prevention and detection of unlawful activities including fraud, whistleblowing, and network and information security, where it may not be possible to take consent in all situations. Resorting to consent in such situations, as a ground for processing may prove burdensome and may raise concerns of consent fatigue among data principals. Furthermore, relying on consent may hinder the evolution of new technologies relying on data analytics, which may hold significant benefits.³³⁸

(b) Scope

Various processing activities may fall under the ground for reasonable purpose, ranging from processing for the benefit of the data principal to processing for the mutual benefit of the data principal and the data fiduciary.³³⁹ The need for this ground can be broadly understood through the following illustrations:³⁴⁰

- (i) Fraud prevention: An insurance company wishes to process personal data for anti-fraud measures. Seeking consent of the concerned individuals could

³³⁷ See UK Information Commissioner’s Office, Legitimate Interests available at <<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/>> (last accessed on 3 April, 2018). Legitimate interests (as the EU GDPR refers to this ground of processing) is the most flexible lawful basis for processing.

³³⁸ Federico Ferretti, Data Protection and the Legitimate Interest of Data Controllers: Much Ado about Nothing or the winter of Rights? 51 Common Market Law Review (2014); Article 6(f) read with Recital 47, EU GDPR. The ‘reasonable interest’ formulation is similar to EU GDPR’s legitimate interests test with some modifications.

³³⁹ See Data Protection Network, Guidance on the Use of Legitimate Interests under the EU General Data Protection Regulation available at <https://iapp.org/media/pdf/resource_center/DPN-Guidance-A4-Publication.pdf> (last accessed on 27 March 2018) at p. 10.

³⁴⁰ Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller (2014).

- defeat the purpose of such processing. However, conducting such an anti-fraud exercise would be beneficial for both the data fiduciaries as well as the data principals. Therefore, the company would be justified in proceeding under the ground of ‘reasonable purpose’.³⁴¹
- (ii) Credit Scoring: A credit card company will share personal data of its customers with credit reference agencies for credit scoring. Here proceeding under ‘reasonable purpose’ instead of ‘consent’ may be more appropriate if the credit score of individuals is needed to determine creditworthiness and there is an absence of real choice for the data principals.³⁴²

Although consent can cover a large gamut of issues, there is a need for a reasonable purpose test in order to cover certain other residuary purposes as listed above.

However, the any freely constituted residuary ground would be too capacious. Its analogous scope in other jurisdictions like the EU demonstrates an inherent lack of standards and uniformity in application, coupled with the possibility of conflict of interests of the data fiduciary.³⁴³ Its existence as a standalone ground for processing appears to be designed to provide latitude to data fiduciaries, without entirely securing the rights of data principals.³⁴⁴ This may be remedied under the Indian data protection law by circumscribing the ambit of the provision. A list of activities including prevention and detection of unlawful activity like fraud, whistleblowing, mergers and acquisitions, network and information security, credit scoring, and recovery of debt, can be whitelisted by the DPA to guide data fiduciaries. In doing so, the DPA should consider the following factors: the data fiduciary’s interest in processing for that purpose, whether it is possible to obtain consent of the data principal, public interest in the processing for that purpose, effect on the rights of the data principal, and the reasonable expectations of the data principal in the context of the processing.

Regardless of the scope of processing, the fundamental rights of data principals should be balanced with the interests of the data fiduciary. This balancing exercise should be done by the DPA in a neutral manner. Further, in order to ensure transparency, data principals should be notified by the data fiduciaries if processing is taking place under this ground.

Processing of personal data made public by a data principal also falls into this category. Conventional views of privacy would offer little protection to such information made public by an individual as the act of making information publicly available could be said to denude the individual of any reasonable expectation of privacy. In the United States, for example,

³⁴¹ Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller (2014).

³⁴² UK Information Commissioner’s Office, Consultation: GDPR consent guidance available at <https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf> (last accessed on 27 March, 2018) at p. 13.

³⁴³ Paolo Balboni et al., Legitimate Interest of the Data Controller New Data Protection Paradigm: Legitimacy Grounded on Appropriate Protection, 3(4) International Data Privacy Law (2013) at p. 250.

³⁴⁴ Paolo Balboni et al., Legitimate Interest of the Data Controller New Data Protection Paradigm: Legitimacy Grounded on Appropriate Protection, 3(4) International Data Privacy Law (2013) at p. 251.

courts have responded to claims of privacy in such information by developing doctrines such as the “third-party doctrine”³⁴⁵ or the “plain view doctrine”³⁴⁶ which grant limited or no protection to information made available to third parties or which is available at a publicly accessible place. The internet provides easily accessible fora including social networking sites where personal data is published or disseminated by data principals. The conventional American approach has been acknowledged to be ill-suited for disclosure of personal data over the internet.³⁴⁷

In India, the third-party doctrine has been rejected by the Supreme Court in *District Registrar v. Canara Bank*³⁴⁸ where the Court noted that documents shared voluntarily with a bank continue to remain confidential vis -à-vis the person, even if they are no longer at the customer's house. This view seems to be closer to the European idea that an individual in spite of any voluntary sharing of, or the disclosure of information would retain an expectation of privacy.³⁴⁹

Accepting this approach would also require acknowledging and balancing other societal interests including the rights of third parties. Any strict rule limiting the processing of data made public may impede free speech related to such data on the internet. This problem may be even more significant in the case of public figures where third parties may have a right not only to process personal data made public by the concerned individual but also personal data emanating from other sources including journalistic activities.³⁵⁰

On the other hand, limits of fair processing must also be clearly drawn. While an individual making personal data, public may have a lower expectation of privacy, it is unlikely that every kind of disclosure is made with the expectation that personal data may be used for profiling whether by private entities or by the state. In addition to immediate privacy harms to the individual resulting from profiling, leaving personal data made public to be freely subject to data analytics and profiling may have the effect of chilling free speech and social interaction through the use of electronic means. The balancing exercise is further complicated

³⁴⁵ United States v. Miller, 425 U.S. 435, 442 (1976); this approach is slowly being revisited in the US while recognising that the Fourth Amendment Standards are ill-suited to sharing of information over the internet.

³⁴⁶ California v. Ciraolo, 476 U.S. 207, 211-12 (1986).

³⁴⁷ In United States v. Jones, 132 S. Ct. 945, 957 (2012), Sotomayer, J. observed that the approach is “ill-suited to the digital age, in which people reveal a great deal about themselves to third parties in the course of carrying out mundane tasks.” See also, Joel Reidenberg, Privacy in Public, 69 University of Miami Law Review (2014).

³⁴⁸ (2005) 1 SCC 496 (note, however, that this was discussed in relation with questions of confidentiality of data shared with a bank and not strictly in relation with personal data disclosed publicly).

³⁴⁹ See Case of von Hannover v. Germany [2004], Judgment, European Court of Human Rights (Application no. 59320/00), at paragraph 77: “the Court considers that the public does not have a legitimate interest in knowing where the applicant is and how she behaves generally in her private life even if she appears in places that cannot always be described as secluded and despite the fact that she is well known to the public”; for a discussion on the difference between the American and European approaches on this point, see Daniel J. Solove and Neil M. Richards, Privacy’s Other Path: Recovering the Law of Confidentiality, 96 Georgetown Law Journal (2007).

³⁵⁰ For further discussion on the processing of data by journalists, see section on journalistic purposes in Chapter 8 of this report; see also, Barrymore v. News Group Newspapers, Ltd. [1997] F.S.R. 600 (Ch.) (U.K.) (discussing issues related to intimate relationships of public personalities) and Florida Star v. BJF, 491 US 524 (1989) (discussing the publication by a newspaper of the name of a rape victim inadvertently disclosed in government records).

by the variety of platforms on the internet. These can range from platforms that permit public disclosures to platforms that facilitate more limited disclosures (such as through a private profile on a social networking site).³⁵¹

It should be noted that the right to be forgotten (discussed in Chapter 5) constitutes a limited response to the problem of personal data available in public. Beyond this, the need for a continuing balancing exercise points to the fact that this processing must be categorised as a reasonable purpose for which the DPA can whitelist permitted actions while maintaining appropriate safeguards.

(c) Application of Obligations

If processing is undertaken under this ground a data fiduciary must comply with all obligations under the data protection law, with the exception of consent, which will not have to be obtained.³⁵² Further, in the case of activities such as whistleblowing, fraud prevention or routine processing of publicly available data in the exercise of free speech where the obligation to give notice may impede the object of the processing, the DPA may consider exempting the requirement of notice. The DPA is also required to put in place appropriate safeguards or conditions whenever it whitelists a reasonable purpose.

Exemptions

A. White Paper and Public Comments

The White Paper suggested that exemptions may be provided from data processing for household purposes, journalistic/artistic and literary purposes, academic research, statistics and historical purposes, investigation and prosecution of crime, maintenance of national security and public order.³⁵³ Further, it was felt that exemptions should have sufficient safeguards, such as only allowing processing for the stated purpose, while ensuring that they were reasonable and not granted arbitrarily. Further, they should have an effective review mechanism in place.³⁵⁴ A large number of commenters agreed with the need for exemptions in the law. One commenter suggested limited number of exemptions and avoiding delegated

³⁵¹ Such distinctions acknowledge that the legal protection of privacy is not just towards the protection of secrecy but also towards control over the degree of accessibility of data shared. See, for a discussion on this point in relation with the US Freedom of Information Act, Daniel J. Solove, Conceptualizing Privacy, 90(4) California Law Review (2002) at p.1109.

³⁵² More specifically, the requirements of necessity, proportionality and purpose limitation. See Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller (2014).

³⁵³ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 59.

³⁵⁴ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 59.

legislation as guiding principles in determining exemptions, which would also ensure that the discretionary power of the DPA is restricted.³⁵⁵

While a majority of commenters supported an exemption for domestic/personal activities, mixed responses were received on the exemption related to research. Some commenters expressed a view that innovation is an important and legitimate purpose of the state and its subjects. However, there was a general view that the question of balancing this purpose with the right to privacy of individuals is a sensitive call and must be examined in the larger societal and commercial context of research, innovation and advancement.

A number of commenters supported the incorporation of the exemption related to national security. However, a majority of commenters expressed concerns related to roadblocks in implementation, and potential misuse by the state. It was suggested that the text of the legislation must ensure that the exemption in this category is used for a *bona fide* purpose. Further, the law should incorporate strict security safeguards and clearly defined obligations on state agencies. Commenters also highlighted the need for guarding against unfettered state surveillance, and the need for an effective review mechanism and adequate judicial oversight for national security tasks.

B. Analysis

For the creation of a truly free and fair digital economy, it is vital to provide certain exemptions from obligations that will facilitate the unhindered flow of personal data in certain situations. These exemptions derive their necessity from either a state or societal interest. However, these exemptions must be limited to processing that is necessary and proportionate to the purpose sought to be achieved. The data protection law must carefully outline watertight exemptions that are narrow and are availed in limited circumstances. Further, adequate security safeguards must be incorporated in the law to guard against potential misuse. We have identified security of the state;³⁵⁶ prevention, detection, investigation and prosecution of contraventions of law;³⁵⁷ processing for the purpose of a legal proceeding; research purposes;³⁵⁸ personal or domestic purposes; manual processing by small entities; and journalistic purpose³⁵⁹ as interests which should be privileged with exemptions from certain obligations of the law. As mentioned in the introduction to this chapter, these exemptions will differ in degree and shall operate in a limited manner. The scope and rationale for each of these exemptions is discussed in the relevant sections below.

³⁵⁵ Comments in response to the White Paper submitted by Supratim Chakraborty, Associate Partner at Khaitan & Co. on 31 January 2018, available on file with the Committee.

³⁵⁶ *Justice KS Puttaswamy & Anr v. Union of India & Ors* (2017) 10 Scale 1 at page 255 (Chandrachud, J.), at page 38 (Sanjay Kishan Kaul, J.).

³⁵⁷ *Id* at page 256 (Chandrachud, J.).

³⁵⁸ *Id* at page 38 (Sanjay Kishan Kaul, J.)

³⁵⁹ *Id* at page 38 (Sanjay Kishan Kaul, J.) Generally talks about how the right to privacy should be balanced with other fundamental rights.

I. Security of the State

(a) Context

A potent threat to the effectiveness of any data protection framework lies in its permissiveness towards exempting the application of fundamental principles on the grounds of national security. National security is a nebulous term, used in statutes of several jurisdictions to denote intelligence gathering activities that systematically access and use large volumes of personal data.³⁶⁰ The ostensible purpose of such processing is to continuously gather intelligence to prevent attacks against the country, whether internal or external. Though always an incident of state power, the pervasiveness of such intelligence gathering has significantly expanded in the data economy.³⁶¹ It is thus critical to ensure that the pillars of the data protection framework are not shaken by a vague and nebulous national security exception.

It is nobody's case that processing for national security is an illegitimate state interest; it undoubtedly is legitimate, and has been recognised by the Supreme Court of India as such.³⁶² The key question is what safeguards can be instituted to ensure that the use of this ground is restricted to genuine cases of threats to national security.

The core case for a national security exemption to data protection law arises in the scenario where personal data of targeted individuals is sought in order to prevent a potential threat. It is common sense that in such a case, where information collection and processing requires to be secret and expedited, standard grounds for processing would not apply. Further, since there is no principal-fiduciary relationship in this case, rights of individuals and obligations of entities would be similarly inapplicable. Periodic review alone can ensure that the personal data sought was indeed used for a legitimate national security purpose and not otherwise.

Such a core case however is at odds with how processing of personal data for national security purposes actually works in practice. Contrary to the case-by-case approach on which the core case is premised, intelligence gathering for national security purposes is premised on systematic government access. Systematic government access is understood as direct access by the government to large volumes of personal data held by private sector entities.³⁶³ The

³⁶⁰ Article 29 Working Party Opinion, Working Document on Surveillance of Electronic Communications for Intelligence and National Security Purpose (2014) available at <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf> (last accessed on 20 April 2018) at pp. 22-25.

³⁶¹ National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law, Directorate General of Internal Policies – Civil Liberties, Justice and Home Affairs, European Parliament (2013) available at <http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET%282013%29493032_EN.pdf> (last accessed on 16 May 2018).

³⁶² See *Puttaswamy*, (2017) 10 SCALE 1 at page 255 (Chandrachud, J.), at page 38 (Sanjay Kishan Kaul, J.). Further, national security restrictions on rights were upheld in the context of the Terrorist and Disruptive Practices (Prevention) Act, 1987 in *Kartar Singh v. State of Punjab*, (1994) 3 SCC 569 and the Prevention of Terrorism Act, 2002 in People's Union for Civil Liberties (PUCL) v. Union of India, (2004) 9 SCC 580.

³⁶³ See Ira Rubinstein et al, Systematic Government Access to Personal Data: A Comparative Analysis, 4(2) International Data Privacy Law (2014).

revelations by Edward Snowden demonstrated the reality of systematic access by the National Security Agency to personal data held on servers of private companies in the US.³⁶⁴ However, this is a practice not limited to the US alone — a survey of 13 countries demonstrated its widespread prevalence in the world, including most leading democracies.³⁶⁵

In this context, it becomes all the more critical to determine the meaning of the term ‘national security’. *Prima facie*, the term itself is alien to Indian constitutional law.³⁶⁶ Article 19(2), which justifies certain restrictions on freedom of speech and expression, uses the phrase ‘security of the State’ instead.³⁶⁷ The Supreme Court has understood this term to mean ‘anything tending to overthrow the State’.³⁶⁸ Certain aggravated instances of public disorder have also been held to affect the security of the state.³⁶⁹ Further, it has been held to include armed rebellion, leaking information to foreign countries and disaffection in the armed forces, paramilitary or police.³⁷⁰ Several other statutes use this ground to restrict fundamental rights.³⁷¹ It is apparent that what the Constitution understands as ‘security of the State’ is in common legal parlance today, understood as ‘national security’.

In our view, seven decades of jurisprudence provides good reason to adopt the term ‘security of the state’ in place of ‘national security’ as an exemption to the fundamental principles of the data protection framework. ‘National security’ is undefined in every jurisdiction we have studied, and much criticism has been made of this lack of definition.³⁷² Using ‘security of the state’ provides greater certainty of which matters can, and cannot, be included as legitimate grounds for exempting the application of data protection principles, based on existing precedent. Further, implicit in this understanding of ‘security of the state’ is the indication of gravity of the act, as it must be of a nature that tends to overthrow the state itself or affect its security fundamentally. No like indication of gravity is implicit in ‘national security’ since little jurisprudence has developed.

Having established ‘security of the state’ as the ground for partial exemption of the data protection law, it is important that certain safeguards to prevent abuse are considered. From the perspective of maintaining the sanctity of the data protection framework, the existing

³⁶⁴ This systematic access programme is commonly referred to as the PRISM programme.

³⁶⁵ Such countries include UK, Germany, France and India, see Ira Rubinstein et al, *Systematic Government Access to Personal Data: A Comparative Analysis*, 4(2) *International Data Privacy Law* (2014).

³⁶⁶ There is however the National Security Act, 1980. While it uses the term “national security” in its title and text (“Security of India” in Section 3), it is not relevant to our purpose as it deals only with preventive detention.

³⁶⁷ Generally, courts have been extremely deferential to the understanding of the executive in its interpretation of a restriction on fundamental rights on the ground of ‘security of the state’. See for example, *Kartar Singh v. State of Punjab*, (1994) 3 SCC 569.

³⁶⁸ *Santokh Singh v. Delhi Administration*, 1973 AIR SC 1091.

³⁶⁹ *Brij Bhushan v. State of Delhi*, 1950 AIR SC 129.

³⁷⁰ *Union of India v. Tulsiram Patel*, 1985 AIR SC 1416.

³⁷¹ Section 5, *Telegraph Act*; and Section 69, *IT Act*.

³⁷² “Despite this, most laws simply list ‘national security’ as a ground for restricting access to information without defining this term at all, let alone providing a specific list of categories of exceptions. In many cases, these laws do not even require the disclosure to pose a risk of harm to national security.” Toby Mendel, *The Johannesburg Principles: Overview and Implementation* available at <<https://www.article19.org/data/files/pdfs/publications/jo-burg-principles-overview.pdf>> at p. 15; See generally Melvyn P. Leffler, *National Security*, 77 *The Journal of American History* (1990).

methods of non-consensual interception and access to personal data in law have to be taken into account and safeguards against misuse scrutinised.

The design of the current legal framework in India is responsible for according a wide remit to intelligence and law enforcement agencies. At the same time, it lacks sufficient legal and procedural safeguards to protect individual civil liberties.³⁷³ Much intelligence-gathering does not happen under the remit of the law, there is little meaningful oversight that is outside the executive, and there is a vacuum in checks and balances to prevent the untrammeled rise of a surveillance society.

There is no general law in India today that authorises non-consensual access to personal data or interception of personal communication for the purposes of intelligence gathering or national security. If there are any entities that are carrying out activities of such a nature without statutory authorisation (for example, solely through executive authorisation), such activities would be illegal as per the *Puttaswamy* judgment as they would not be operating under law. The Intelligence Services (Powers and Regulation) Bill, 2011 had been introduced to regulate the manner of functioning of Indian intelligence agencies and institute an oversight mechanism.³⁷⁴ However, the Bill lapsed in 2011 and left the legislative vacuum unaddressed.

However, for at least some of the instances of monitoring and interception, access to personal data is currently obtained through certain statutory provisions.³⁷⁵ For instance, the Telegraph Act authorises interceptions in the interests of the security of the state if the Central Government, State Government or a special officer are satisfied that it is both ‘necessary and expedient’.³⁷⁶ Similarly, under the IT Act, the Central Government may issue directions for monitoring, interception or decryption of information transmitted, received or stored on a computer device, when it is necessary or expedient in the interest of security of the state.³⁷⁷ Further in the interest of cyber security, the Central Government may authorise an agency to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource. All persons must comply with the directions of such authorised agency to avoid imposition of penalty.³⁷⁸

³⁷³ NIPFP Technology Policy, Use of personal data by intelligence and law enforcement agencies, June 27, 2018, p. 4.

³⁷⁴ Manish Tewari, State of the Union: Time for intelligence reforms?, *Deccan Chronicle*, 19 March 2016, available at <https://www.deccanchronicle.com/opinion/op-ed/190316/state-of-the-union-time-for-intelligence-reforms.html>; See NIPFP Technology Policy, Use of personal data by intelligence and law enforcement agencies, June 27, 2018, p. 4.

³⁷⁵ This is not an exhaustive analysis. Other provisions in central and state laws may exist for access for specific purposes. For instance, Section 33, Aadhaar Act permits the disclosure of information by order of a court not inferior to that of a District Judge.

³⁷⁶ Section 5, Telegraph Act.

³⁷⁷ Section 69, IT Act.

³⁷⁸ Section 69B, IT Act.

For each of these mechanisms, oversight is carried out through a Review Committee set up under the Telegraph Rules.³⁷⁹ This Committee reviews interception orders passed under the Telegraph Act³⁸⁰ and Section 69B of the IT Act. It consists of the Cabinet Secretary, Secretary to the Government of India in charge of Legal Affairs and the Secretary to the Government of India in charge of Department of Telecommunications. As per a recent RTI application to the Ministry of Home Affairs, it has been found that about 7500-9000 such orders are passed by the Central Government every month.³⁸¹ The Review Committee has an unrealistic task of reviewing 15000-18000 interception orders in every meeting, while meeting once in two months.³⁸²

Additionally, surveillance practices are also enabled by the license agreements entered into by telecom service providers with the Government.³⁸³ For example, such agreements can mandate low encryption standards. This poses a threat to safety and security of the personal data of data principals.

Surveillance should not be carried out without a degree of transparency that can pass the muster of the *Puttaswamy* test of necessity, proportionality and due process.³⁸⁴ This can take various forms, including information provided to the public, legislative oversight, executive and administrative oversight and judicial oversight.³⁸⁵ This would ensure scrutiny over the working of such agencies and infuse public accountability.

Executive review alone is not in tandem with comparative models in democratic nations which either provide for legislative oversight, judicial approval or both. Legislative oversight exists in Germany; judicial review in UK; and some form of both in South Africa. At the same time, it is instructive to note that the data protection legislations in each of these countries dovetail with each substantive legislation relating to national security.

Thus, in South Africa, under the Intelligence Services Oversight Act, 1994³⁸⁶ there is a parliamentary as well as civil oversight mechanism which together hold security structures accountable and receives complaints about intelligence services. Further, the Regulations of

³⁷⁹ Rule 419A (16), Telegraph Rules.

³⁸⁰ Section 5(2), Telegraph Act.

³⁸¹ Comments in response to the White Paper submitted by Kalyan Biswas, Associate Vice President at Internet and Mobile Association of India on 31 January 2018, available on file with the Committee.

³⁸² Comments in response to the White Paper submitted by Kalyan Biswas, Associate Vice President at Internet and Mobile Association of India on 31 January 2018, available on file with the Committee.

³⁸³ NIPFP Technology Policy, Use of personal data by intelligence and law enforcement agencies, June 27, 2018, p. 11.

³⁸⁴ NIPFP Technology Policy, Use of personal data by intelligence and law enforcement agencies, June 27, 2018, p. 21-23.

³⁸⁵ NIPFP Technology Policy, Use of personal data by intelligence and law enforcement agencies, June 27, 2018, p. 21-23.

³⁸⁶ The Intelligence Services Oversight Act, 1994, see statement of objects and reasons – “To provide for the establishment of a Committee of Members of Parliament on Intelligence and to define its functions; and for the appointment of Inspectors General or Intelligence and to define their functions; and to provide for matters connected therewith.” available at <<https://oldsite.issafrica.org/uploads/INTELSERVACT40OF1994.PDF>> (last accessed on 19 April 2018).

Interception of Communications and Provision of Communication-related Information Act, 2000³⁸⁷ requires judicial approval for interception of communication activities. The POPI Act exempts personal data involving national security³⁸⁸ from its purview to the “the extent that adequate safeguards have been established in legislation for the protection of such personal information.”³⁸⁹

In Germany, the Parliamentary Control Panel appointed under the Act on the Control of the Intelligence Activities of the Federation, 1978 scrutinises intelligence activities.³⁹⁰ Comprehensive information on intelligence activities is released to this panel which then reports to the Parliament. Further, administrative control exists in the form of the relevant federal ministries exercising supervision over the intelligence agencies under them and the Federal Commissioner of Data Protection and Freedom of Information who monitor compliance of the federal intelligence agencies with the data protection laws.³⁹¹ The Federal Data Protection Act allows for derogation from the data protection law if a public body needs to process personal data “necessary to prevent a substantial threat to public security or necessary for urgent reasons of defence.”³⁹²

In UK, under the Investigatory Powers Act³⁹³ interception warrants can be issued by the Secretary of State upon application by an interception authority which further require approval by the Judicial Commissioner to ensure that the tests of proportionality and necessity were met at the time of issuance of the warrant. The UK DPA exempts personal data required for the purpose of safeguarding national security from the principles of data protection as well as the rights and obligations set out under the law.³⁹⁴

In the US, the oversight mechanisms primarily exist in the form of various Congressional committees and mechanisms under the executive office of the President.³⁹⁵ The House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence

³⁸⁷ The Regulations of Interception of Communications and Provision of Communication-related Information Act, 2000 available at <<https://www.justice.gov.za/legislation/acts/2002-070.pdf>> (last accessed on 19 April 2018).

³⁸⁸ Section 6(1) (c), POPI Act. The term “national security” has been expanded upon as “including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defence or public safety”.

³⁸⁹ Section 6(1)(c), POPI Act.

³⁹⁰ Foreign Intelligence Gathering Laws: Germany, Library of Congress available at <<https://www.loc.gov/law/help/intelligence-activities/germany.php>> (last accessed on 9 May 2018).

³⁹¹ Foreign Intelligence Gathering Laws: Germany, Library of Congress available at <<https://www.loc.gov/law/help/intelligence-activities/germany.php>> (last accessed on 9 May 2018).

³⁹² Section 22, Federal Data Protection Act. Further, Section 23, Federal Data Protection Act allows for processing of personal data apart from the purpose collected if the data if the “processing is necessary to prevent substantial harm to the common good or a threat to public security, defence or national security”.

³⁹³ Section 138, Investigatory Powers Act.

³⁹⁴ Section 28, UK DPA.

³⁹⁵ Oversight of the Intelligence Agencies: a comparison of the ‘Five Eyes’ Nations (2017), Parliamentary Library, Parliament of Australia available at <http://parlinfo.aph.gov.au/parlInfo/download/library/prspub/5689436/upload_binary/5689436.pdf>.

are the primary intelligence oversight bodies.³⁹⁶ Judicial oversight exists under the FISA for *ex ante* judicial approvals for gathering foreign intelligence.³⁹⁷

Though each of these jurisdictions provides for external oversight over executive intelligence actions, such mechanisms have been widely criticised as being ineffectual. Thus, in the US, FISA courts have granted 99.97% of all applications.³⁹⁸ Though by itself this may not determine permissiveness, since, it is argued that the executive may be self-selecting,³⁹⁹ nonetheless, the acceptance rate is unquestionably high. At the same time, the secret nature of the proceedings means that there is no way of knowing whether the review was indeed fair. Most crucially, judicial approvals for mass intelligence gathering appears to be an example of a category mistake—a form of review more suitable for particularised decision-making being used to authorise systematic access renders remote the possibility of genuine case-by-case approval.

On the other hand, legislative oversight too is subject to considerable criticism. For instance, the Parliamentary Control Panel in Germany has been criticised because its membership solely constitutes of Members of Parliament and they lack the time to study the information in depth.⁴⁰⁰ Further, they have no means of verifying the information supplied by the government.⁴⁰¹ Congressional oversight in US has been criticised as being ritualistic and being akin to a ‘security theatre’ with the vast amounts of information being supplied to the Congress entering a Congressional void.⁴⁰²

Despite these criticisms, it is worthwhile to recognise that all the aforementioned jurisdictions provide some form of inter-branch oversight through a statute. Nothing similar exists in India. This is not just a gap that is deleterious in practice but, post the judgment of the Supreme Court in *Puttaswamy*, potentially unconstitutional. This is because the Supreme Court has clearly laid down that any restriction of the right to privacy must satisfy three tests: first, the restriction must be by law, second, it must be necessary and proportionate and third, it must promote a legitimate state interest.⁴⁰³ The salience of procedural safeguards within the interception structure has also been emphasised to prevent abuse. Though the nature of the intelligence gathering in a particular case will have to be carefully scrutinised to ascertain

³⁹⁶ Oversight of the Intelligence Agencies: a comparison of the ‘Five Eyes’ Nations (2017), Parliamentary Library, Parliament of Australia available at <http://parlinfo.aph.gov.au/parlInfo/download/library/prspub/5689436/upload_binary/5689436.pdf>.

³⁹⁷ Sections 103 (a)(1) and 103(b), FISA.

³⁹⁸ Conor Clarke, Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp? Ex Parte Proceedings and the FISC Win Rate, 66 Stanford Law Review Online (2014).

³⁹⁹ Conor Clarke, Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp? Ex Parte Proceedings and the FISC Win Rate, 66 Stanford Law Review Online (2014).

⁴⁰⁰ Alvar Freude and Trixy Freude, Echoes of History: Understanding German Data Protection, Bertelsmann Foundation available at <<http://www.bfna.org/research/echos-of-history-understanding-german-data-protection/>> (last accessed on 9 May 2018).

⁴⁰¹ Alvar Freude and Trixy Freude, Echoes of History: Understanding German Data Protection, Bertelsmann Foundation available at <<http://www.bfna.org/research/echos-of-history-understanding-german-data-protection/>> (last accessed on 9 May 2018).

⁴⁰² See P. M. Schwartz, Reviving Telecommunication Surveillance Law, 75(1) University of Chicago Law Review (2008) at p. 310.

⁴⁰³ *Puttaswamy*, (2017) 10 SCALE 1 at para 180.

whether it satisfies the second and third tests, several types of current intelligence gathering in India falls at the first threshold, since it is not done under law. Further, statutorily recognised interceptions may also require further scrutiny as to whether they are indeed necessary or proportionate, which are new standards for fundamental rights restrictions to satisfy post *Puttaswamy*.

(b) Scope

It is the Committee's view that the data protection law must contain adequate safeguards to adhere strictly to the judgment of the Supreme Court in *Puttaswamy*. The data protection law will enable an exemption to the processing of personal or sensitive personal data if it is proportionate and necessary in the interest of the security of the state and is pursuant to a law that meets the test of constitutionality. Further, any restriction on privacy must be proportionate and narrowly tailored to the stated purpose. Finally, obligations on maintaining security safeguards in processing personal data will remain on the agency collecting such data and no exemption to the same will be provided.

Following the precedents in other jurisdictions, we also recommend that the Central Government carefully scrutinise the question of oversight of intelligence gathering and expeditiously bring in a law to this effect. Such a law should provide for both parliamentary oversight as well as judicial approval of all requests for non-consensual access to personal data. The key rationale underlying such checks and balances is the need for *ex ante* access control as well as *ex post* accountability. For the former, a district judge may be designated and given security clearance for this purpose in each district to hear such requests and dispose them expeditiously. Given the sensitivity of the matter, such proceedings should be closed-door, with regular reporting to an appropriate parliamentary committee. Further, all such approvals should be time-bound and require renewal on the judge being satisfied that the purpose for processing remains relevant. A periodic review before a parliamentary committee is necessary, where such review should be conducted via closed-door proceedings, as it is done in South Africa.⁴⁰⁴ Ex-ante and post-facto reporting and transparency requirements should also be incorporated in the appropriate law.⁴⁰⁵

The surveillance architecture should also embed systematic risk management techniques within itself.⁴⁰⁶ This would lead to the prioritisation and narrowing of its activities, by devoting resources to credible risks, whether reputational or organisational.⁴⁰⁷ For example, an assessment of whether a particular measure is the least intrusive measure to achieve a

⁴⁰⁴ The Joint Standing Committee on Intelligence in South Africa has oversight over all security structures and oversight bodies which must be accountable to it.

⁴⁰⁵ NIPFP Technology Policy, Use of personal data by intelligence and law enforcement agencies, June 27, 2018, p. 29.

⁴⁰⁶ NIPFP Technology Policy, Use of personal data by intelligence and law enforcement agencies, June 27, 2018, p. 28.

⁴⁰⁷ NIPFP Technology Policy, Use of personal data by intelligence and law enforcement agencies, June 27, 2018, p. 28.

stated aim may be required.⁴⁰⁸ Not only will this reduce costs incurred by the State, it will also be consistent with civil rights protection.⁴⁰⁹

We would hasten to add that this recommendation, albeit not directly made a part of the data protection statute, is important for the data protection principles to be implemented effectively and must be urgently considered.

(c) Application of Obligations

Apart from the obligations of security safeguards and fair and reasonable processing none of the other obligations under the data protection law shall apply to the processing of personal data under the security of state exemption. The collection and processing in such situations by its very nature may be covert and expedited, thereby making consent inapplicable. It therefore flows, that obligations such as purpose specification and storage limitation will also not apply through the proposed data protection law and, if applicable, would be implemented in a modified form through the appropriate statute authorising the intelligence activities. Moreover, since a principal-fiduciary relationship has not been envisaged in this case, rights of the individuals will also not be applicable.

II. Prevention, Detection, Investigation and Prosecution of Contraventions of Law

(a) Context

Prevention, detection, investigation and prosecution of contraventions of law (including disciplinary proceedings and investigation into tax contraventions) are important state functions, central to the protection of individuals and the society at large. It is a legitimate aim of the state.⁴¹⁰ The state enjoys a monopoly of the legitimate use of physical force to enforce order within its sovereign territory.⁴¹¹ The Constitution entrusts State Governments and Union Territories with the maintenance of law and order,⁴¹² including “prevention, detection, registration, investigation and prosecution of crimes.”⁴¹³ While these activities are in pursuance of a legitimate aim of the state, they must meet the test of necessity and proportionality, as laid down in *Puttaswamy*.⁴¹⁴

Law enforcement activities stem from the larger obligations of the state to maintain public order in society. The Committee acknowledges that sometimes the line between situations

⁴⁰⁸ NIPFP Technology Policy, Use of personal data by intelligence and law enforcement agencies, June 27, 2018, p. 28.

⁴⁰⁹ NIPFP Technology Policy, Use of personal data by intelligence and law enforcement agencies, June 27, 2018, p. 28.

⁴¹⁰ *Puttaswamy*, (2017) 10 SCALE 1, Part S, para 181.

⁴¹¹ H.H. Gerth and C. Wright Mills (eds.), *Max Weber: Essays in Sociology* (Oxford University Press, 1946).

⁴¹² Entry 1 and 2, List II, Schedule VII, Constitution of India.

⁴¹³ Response of the Minister of Home Affairs (Government of India) to unstarred question no. 1354 (Lok Sabha) (5 March 2013) available at <<https://mha.gov.in/MHA1/Par2017/pdfs/par2013-pdfs/Is-050313/LSQ.1354.Eng.pdf>> (last accessed on 10 May 2018).

⁴¹⁴ *Puttaswamy*, (2017) 10 SCALE 1.

threatening the security of state and those posing a threat to public order may be blurred.⁴¹⁵ Since law enforcement agencies are also engaged in anticipating and preventing possible attacks, it may become difficult to ascertain when a disorder will constitute a mere crime and when it may transcend to a threat to national security. The term “public order” has been understood to mean less aggravated forms of disorder that disturb public peace and tranquillity in comparison to endangering the “security of state”.⁴¹⁶ Accordingly, the data protection law should distinguish between exemptions provided for the purpose of national security and law enforcement.

The focus of law enforcement activities of police, investigating authorities and revenue authorities is on individuals. Consequently, a significant amount of personal data is processed while undertaking these activities. Courts in India have often had to resolve the continuous conflict between issues of spatial and informational privacy, liberty and autonomy of the individuals, while ensuring safety of citizens through law enforcement.⁴¹⁷ In this context, it is critical for a data protection law to effectively address concerns relating to the right to privacy of individuals, and at the same time ensure that crucial state functions are not impeded. Data protection laws across jurisdictions have carved out specific exemptions for processing related to prevention, detection, investigation and prosecution of contraventions of law.⁴¹⁸

As per the RTI Act, information which would impede the process of “investigation or apprehension or prosecution of offenders” is exempted from being disclosed to any citizen.⁴¹⁹ The phrase has been interpreted to include investigation during disciplinary proceedings, investigation by income tax authorities, etc. While there is no watertight definition of the terms “investigation” or “prevention and detection of crime”, a perusal of criminal legislation in India lends sufficient clarity. The CrPC provides an inclusive definition of the term ‘investigation’ to mean all proceedings under the CrPC for the “collection of evidence conducted by a Police officer or by a person (other than a Magistrate) who is authorised by a Magistrate in this behalf”.⁴²⁰

The procedural aspects regarding the recording of crimes, investigation of criminal cases and execution of arrest, search and seizure are dealt with under the CrPC. It contains detailed provisions on arrest to stipulate when a police officer can make an arrest without a warrant⁴²¹ or on refusal to furnish name and address,⁴²² arrest by private person,⁴²³ arrest by

⁴¹⁵ It is relevant to note the theory of “three concentric circles”, i.e. “law and order” (largest), “public order” and “security of state” (smallest), as discussed in *Ram Manohar Lohia v. State of Bihar*, AIR 1966 SC 740.

⁴¹⁶ *Romesh Thapar v. State of Madras*, AIR 1950 SC 124.

⁴¹⁷ *Directorate of Revenue v. Mohammad Nisar Holia*, (2008) 2 SCC 370 at para 14; *People’s Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC at para 18; *ITO v. Seth Bros.*, (1969) 2 SCC 324 at para 8; *Bai Radha v. State of Gujarat*, (1969) 1 SCC 43 at para 10.

⁴¹⁸ See Section 29, UK DPA; Clauses 31 and 43(3), UK Data Protection Bill; Section 6(1)(c)(ii), Sections 15(3)(c)(i), 18(4)(c)(i), 22(3), 37(2)(b), POPI Act.

⁴¹⁹ Section 8(1) h, RTI Act.

⁴²⁰ Section 4(h), CrPC.

⁴²¹ Section 41, CrPC.

⁴²² Section 42, CrPC.

Magistrate⁴²⁴ etc., as well as how such arrest should be made.⁴²⁵ Under Section 91 of the CrPC, an officer in charge of a police station can require a person, by written order, to produce a document or any other thing that is “necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under this Code”. As per the CrPC, an investigation may also include the ascertainment of facts and circumstances of a case, search and arrest of a suspected offender, search of the premises and seizure of material important to the investigation, examination of various individuals relevant to the case etc.⁴²⁶ In all these stages, personal data is processed by the police.

The PMLA grants powers of search and seizure to an authorised officer.⁴²⁷ Here, the authorised officer may seize any record or property found during the course of search, and retain the seized property or record if the retention is necessary for an inquiry.⁴²⁸ The NIA Act is geared towards curbing terror attacks, militancy and insurgency. It provides wide powers to investigate connected offences along with scheduled offences.⁴²⁹ Further, apart from police investigations, regulators like the SEBI and the CCI grant powers to investigating authorities to search places,⁴³⁰ seize books, registers, documents and records,⁴³¹ keep such information in custody,⁴³² conduct inquiries into alleged contravention of the applicable law,⁴³³ and conduct inquiries into disclosures made.⁴³⁴

The Income Tax Act also provides powers to the state authorities to make enquiries or investigate whether income has been concealed towards the protection of revenue.⁴³⁵ Their powers of enquiry and investigation also extend to any persons or class of persons in relation to an agreement entered into by the Central Government with a territory outside India,⁴³⁶ as specified under the Income Tax Act. Further, authorities under the Income Tax Act also have powers to conduct raids,⁴³⁷ search and seizure,⁴³⁸ call for information,⁴³⁹ etc. Disclosure of an assessee’s information may be made to other authorised officials of the Central Government if it is necessary in public interest.⁴⁴⁰ In these instances, tax authorities are compelled to process personal data in compliance with law.

⁴²³ Section 43, CrPC.

⁴²⁴ Section 44, CrPC.

⁴²⁵ Section 46, CrPC.

⁴²⁶ H.N. Rishbud v. State of Delhi, 1955 AIR SC 196.

⁴²⁷ Section 17, PMLA.

⁴²⁸ Section 20 and 21, PMLA.

⁴²⁹ Section 8, NIA Act.

⁴³⁰ Section 11C, SEBI Act.

⁴³¹ Section 11C, SEBI Act.

⁴³² Section 11C, SEBI Act.

⁴³³ Section 19, Competition Act.

⁴³⁴ Section 30, Competition Act.

⁴³⁵ Section 131, Income Tax Act, 1961

⁴³⁶ Sections 90 and 90A, the Income Tax Act.

⁴³⁷ Section 132A, Income Tax Act.

⁴³⁸ Section 132A, Income Tax Act.

⁴³⁹ Section 133, Income Tax Act.

⁴⁴⁰ Section 138, Income Tax Act.

Activities in furtherance of prevention, detection, investigation and prosecution of contraventions of law carried out by law enforcement and revenue agencies may involve processing of personal data as well as sensitive personal data, including DNA samples, biometrics, and official identification documents. Further, advancements in technology have led to significant changes in data collection methods adopted. Given the wide range of powers that law enforcement and revenue agencies enjoy when working towards the prevention, detection, investigation and prosecution of contraventions of law, it is important to verify whether sufficient checks exist on such powers to ensure that they would not unlawfully impinge on the data protection rights of the individuals whose data gets processed in the course of such investigations.

In India, these agencies are subject to parliamentary, executive and judicial oversight as well as scrutiny by other independent statutory bodies.⁴⁴¹

Further, several independent authorities also oversee the functioning of law enforcement agencies to prevent and counteract any abuse of power. For example, the CVC is authorised to receive complaints for and investigate corruption, malpractice or misuse of office allegations.⁴⁴² The CAG audits the accounts of investigatory authorities and therefore checks against the misappropriation of funds.⁴⁴³ The National Human Rights Commission, though without any binding powers, also possesses the authority to probe into alleged human rights violations by the police.⁴⁴⁴ Some states also have a body called the Police Complaints Authority where persons can lodge complaints of ‘serious misconduct’ against the police.⁴⁴⁵

⁴⁴¹ The Parliament through its select committees and department related standing committees periodically reviews laws which provide such powers to law enforcement agencies. See Mario J. Aguja and Hans Born (eds.) DCAF, *The Role of Parliament in Police Governance* (2017) available at <https://www.dcaf.ch/sites/default/files/publications/documents/The_Role_of_Parliament_in_Police_Governance_e.pdf> (last accessed on 10 May 2018). The Executive exercises control over such agencies through the Ministry of Home Affairs which is responsible for all central police forces as well as the Indian Police Service. The Home Minister is also accountable to the Parliament and the relevant State Legislatures. At the local level, the Superintendent of Police is empowered to initiate an inquiry into any complaint made against a subordinate officer. Further, the police force at the district level is placed under the control of the District Magistrates, who also have the power to give guidance to the police (Section 4, Police Act, 1861).

Indian courts have also been proactive in upholding the human rights of Indian citizens against abuses by the police. The Supreme Court, for instance, has come out with guidelines to ensure better accountability for the police and has delivered judgments punishing the police for not following due process or for the abuse of their power (Centre for Law and Policy Research, *Legal Accountability of the Police in India* (2016) available at <<http://clpr.org.in/wp-content/uploads/2016/08/140214-Police-Accountability-website.pdf>> (last accessed on 10 May 2018)). In the case of *Prakash Singh v. Union of India* ((2006) 8 SCC 1), the Supreme Court laid down several means of checks and balances on the powers of the police which included the constitution of State Security Commissions, Police Establishment Boards and Police Complaints Authorities. The Supreme Court had also directed that the investigation wing of the police be separated from the law and order wing to improve investigation time and expertise and further recommended the setting out of a minimum tenure for key police officers. Further, another mechanism of ensuring that the law enforcement agencies do not process personal data that is not strictly necessary for investigation, is by requiring them to obtain search warrants from judicial magistrates (Section 93 CrPC).

⁴⁴² Section 8, Central Vigilance Commission Act, 2003.

⁴⁴³ The powers and functions of the CAG have been laid down in the Comptroller and Auditor General’s (Duties, Powers and Conditions of Service) Amendment Act, 1971.

⁴⁴⁴ Mario J. Aguja and Hans Born (eds.) DCAF, *The Role of Parliament in Police Governance* (2017) available at

Despite these safeguards, it is critical that the principles laid down in the *Puttaswamy* judgment regarding the use of personal data for law enforcement pursuant to a legitimate aim of the state, applied in a necessary and proportionate manner by law need to be followed strictly. The details of application of the principles are contained in (c) below.

(b) Scope

The Committee is of the opinion that the data protection law should provide an exemption for prevention, detection, investigation and prosecution of contraventions of law for both personal as well as sensitive personal data. For this purpose, the specific law enforcement authorities which can claim the use of this exemption would also have to be limited by the data protection law to ensure that there is no scope for the exploitation of vagueness in the law. Further, while the rationale for the provision of this exemption is the maintenance of public order, the term public order must be constrained by specific activities aimed at prevention, detection, investigation and prosecution of crimes, which are constitutional and statutorily derived.

Generally, laws in India grant investigating authorities and the police significant powers to process personal data of individuals. These individuals may be suspects, witnesses, informants, accomplices, victims, offenders and so on. Therefore, personal data of individuals who are not suspected of, or linked to, a crime being investigated should be permitted to be processed only when absolutely necessary for a legitimate and well-defined purpose and only for a limited period of time.⁴⁴⁶

Further, sensitive personal data, should only be processed when strictly necessary for the purposes of a particular inquiry. When processing does take place for such purposes, the data protection law should subject the data fiduciary to more rigorous standards of obligations of security and accuracy. Even within the category of sensitive personal data, which are capable of causing great harm particularly due to their immutable nature, and capacity to automatically identify individuals, should be subject to a greater degree of oversight before their collection.⁴⁴⁷

<[https://www.dcaf.ch/sites/default/files/publications/documents/The Role of Parliament in Police Governance.pdf](https://www.dcaf.ch/sites/default/files/publications/documents/The%20Role%20of%20Parliament%20in%20Police%20Governance.pdf)> (last accessed on 10 May 2018).

⁴⁴⁵ To maintain independence, such a body is to consist of a retired high court judge, and may consist of retired senior level police officer or civil servant. Centre for Law and Policy Research, Legal Accountability of the Police in India (2016) available at <<http://clpr.org.in/wp-content/uploads/2016/08/140214-Police-Accountability-website.pdf>> (last accessed on 10 May 2018).

⁴⁴⁶ Article 29 Working Party Opinion 01/2013 providing further input into the discussions on the draft Police and Criminal Justice Data Protection Directive (2013) available at <http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2013/wp201_en.pdf> (last accessed on 10 May 2018).

⁴⁴⁷ Article 29 Working Party Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (2015) available at <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp233_en.pdf> (last accessed on 10 May 2018).

To avail this exemption with regard to investigation into tax contraventions, processing activities must be carried out strictly in accordance with the relevant statutory provision and the state agency should comply with the obligations and safeguards provided in the statute itself.⁴⁴⁸

(c) Application of Obligations

In instances where law enforcement activities are *bona fide*, and are in pursuance of a legitimate state aim as authorised by law, strict adherence to data protection obligations such as giving privacy notices, providing data principal rights, limiting the use of such data to a particular purpose would impede the purposes sought to be achieved. However, the Committee also recognises that an overbroad exemption in this category may amount to an unreasonable restriction on an individual's right to privacy in certain cases and could defeat the overall objective of a data protection law.

Accordingly, the data protection law should require law enforcement agencies to ensure that processing of personal data is necessary and proportionate to their purposes. For instance, maintenance of a DNA database of all citizens, some of whom may be innocent, to track crime, without legal sanction, would be a disproportionate law enforcement measure. A similar exercise was undertaken in the UK⁴⁴⁹ where subsequently, the government had to delete more than a million records of innocent adults and children after the enactment of the Protection of Freedoms Act, 2012 which *inter alia* regulates the collection, retention, destruction of biometric data, surveillance mechanisms etc.⁴⁵⁰

In most instances, it will be difficult for law enforcement authorities to comply with strict standards of purpose specification. This is because the very nature of investigation is such that the investigator is unaware of the exact manner in which the investigation would be concluded, and subsequently the result of such investigation. Therefore, purpose limitation would not apply where processing of personal data under this exemption is carried out for the prevention, detection, investigation and prosecution of contraventions of law. Whereas purposes may be largely unclear when contraventions are to be prevented or detected (e.g. CCTV surveillance), investigations would still have purposes in a broad sense insofar as the relevant contravention is largely understood. However, this may not meet the standards of purpose specification in the law.

Personal data would however only be collected for the purposes of prevention, detection, investigation and prosecution of contraventions of law. For instance, the local police may

⁴⁴⁸ On the powers of Revenue Officers under Section 132 (Search and Seizure) of the Income Tax Act; ITO v. Seth Brothers, 1969 (2) SCC 324 at para 8.

⁴⁴⁹ Peter M Schneider and Peter D Martin, Criminal DNA Databases: the European Situation, 119 Forensic Science International (2001) at p. 232.

⁴⁵⁰ National DNA Database of UK; see Sujatha Byravan, The Problems with a DNA Registry, The Hindu (8 May 2018) available at <<http://www.thehindu.com/opinion/op-ed/the-problems-with-a-dna-registry/article23805145.ece>> (last accessed on 10 May 2018); see also Margarita Guillén et al, Ethical-Legal Problems of DNA Databases in Criminal Investigation, 26 (4) Journal of Medical Ethics (2000).

collect the name, phone number, and address of the victim and the accused. Seeking information about their religion, caste or tribe may not be relevant to the investigation. However, in order to make a case for collecting information such as their biometrics, the police would be required to ensure that such collection is necessary and proportional to the purpose of investigation.

The obligations of notice and consent ordinarily imposed on data fiduciaries would adversely affect the operation of law enforcement agencies because the coercive powers of these agencies, which may at times impinge on individuals' privacy, are necessary to allow the lawful access to information which would be otherwise unavailable to them. Further, it could lead to problems in obtaining evidence and testimonies from witnesses and may also impede the flow of information between different criminal intelligence agencies.⁴⁵¹ Similarly, providing data principal rights such as access, confirmation, correction, portability and the right to be forgotten would be prejudicial to the law enforcement purpose since it may be necessary to prevent and detect crimes that the suspect is not made aware of an investigation running against him for fear of destruction of evidence.

Processing for investigation into tax contraventions should be exempt from the obligations related to notice, consent, use, and disclosure. This is because compliance with these obligations may defeat the purpose of the statutory provision under which such processing is being carried out. For instance, seeking consent of an individual before conducting search and seizure under the Income Tax Act to ascertain whether there has been a tax evasion, may jeopardise the object of conducting such raids. Similarly, the provision on data principal rights as set out in the data protection law will not apply. In certain instances, personal data may be accessed or rectified subject to the statutory provisions set out in the respective tax and revenue legislation. The obligation of maintenance of security safeguards to ensure safety and integrity of citizens' data should be applicable to officials and authorities discharging such functions.

III. Processing for the purpose of legal proceedings

(a) Context

Non-disclosure provisions in the data protection law will be inapplicable to disclosure of personal data necessary for enforcing any legal right or claim, for seeking any relief, defending any charge, opposing any claim, or obtaining legal advice from an advocate in an impending legal proceeding.

The rationale for exempting the disclosure of personal data in the pursuance of legal claims is to allow data principals to effectively exercise their legal rights under general law, including

⁴⁵¹ See Chapter 37: Agencies with Law Enforcement Functions, Australian Privacy Law and Practice (ALRC Report 108).

the ability to take legal advice from advocates. Applying the obligations under the proposed data protection law may obstruct the realisation of such rights.

Further, processing of personal data by any court or tribunal in India necessary for the exercise of any judicial function will be exempted. This is to cover instances of processing by courts in the performance of their judicial function of resolving disputes brought before it.

(b) Scope

Under the Indian data protection law, disclosure of personal data and sensitive personal data in pursuance of a legal claim would occur if it is required to be produced in connection with any legal proceeding (including in preparation for a legal proceeding to be initiated in the future), or where required to establish, exercise or defend legal rights; or where it is required to be brought to the attention of an advocate for seeking legal advice for an impending legal proceeding. Additionally, processing of personal data by any court or tribunal necessary for the exercise of judicial function shall be exempted.

(c) Application of Obligations

For both disclosure of personal data in pursuance of legal claims and seeking legal advice, as well as processing by any court or tribunal in India for the exercise of any judicial function, the data protection obligations of consent, notice, data principal rights and accuracy will not apply as they may hamper the meaningful exercise of legal rights. However, general obligations with regard to security safeguards and fair and reasonable processing will continue to apply.

IV. Research Activities

(a) Context

The Constitution recognises the development of scientific temper, humanism and the spirit of inquiry and reform as one of the fundamental duties of every Indian citizen.⁴⁵² In order to facilitate this, an exemption for purposes of research has been considered necessary by the Committee to allow for scientific innovation and free flow of ideas and information. In the context of data protection, the need for this exemption arises because certain principles of data protection such as consent, purpose specification, storage limitation and certain data principal rights may not apply, may be at odds with the achievement of research purpose or may prove to be too onerous to fulfil. While in a completely different setting, such exemptions have existed in Indian law in the form of the research exemption in patent law,⁴⁵³ which allows for the uninhibited use of patented articles or processes for research and

⁴⁵² Article 51A (h), Constitution of India.

⁴⁵³ Section 47, Indian Patent Act, 1970.

experimentation.⁴⁵⁴ The intention behind such exemption is to encourage scientific temper and ensure that larger societal interests, such as innovation and spread of knowledge continue without being unduly restricted.⁴⁵⁵

Moreover, such an exemption also operates in pursuance of the constitutional right to free speech and expression.⁴⁵⁶ This is especially true in the context of historical research, where the fundamental right to express oneself may be restricted by rights such as the right to be forgotten, since the epochal quality of information may only become clear long after its creation.⁴⁵⁷ The social good in the exercise of such rights is undeniable since they contribute to the free flow of information and ideas in society.

In academic literature, however, research activities are often viewed in contradistinction to an individual's right to privacy which a data protection law seeks to protect.⁴⁵⁸ In our view, as Valerie Steeves argues, such a formulation is problematic since data protection helps build trust in research practices, mitigates the commercial imperatives that flow from the fact that research is often a public-private enterprise and protect the accuracy of data.⁴⁵⁹ Thus in our approach, research activities and data protection are not viewed as a zero-sum game, but as being complementary to each other.

(b) Scope

In the context of data protection, subject to safeguards, in some form or the other, exemptions for archival purposes in public interest, historical, scientific, and statistical research exist in various jurisdictions.⁴⁶⁰ While this formulation is common, it is important to understand the ambit of these terms in order to justify their exemption from data protection law. The EU GDPR provides guidance on the meaning of these terms. Archival services are understood as being in pursuance of a law that provides the legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest.⁴⁶¹ Scientific research is understood in a broad manner, including technological development and demonstration, fundamental research, applied research, privately funded research and research conducted in the area of public

⁴⁵⁴ For further details, see K. Chakravarthy and N. Pendsey, Research Exemptions in Patent Law, 9 Journal of Intellectual Property Rights (2004) at pp. 332-341.

⁴⁵⁵ Puttaswamy, (2017) 10 SCALE 1 at part T, para 5, recognised innovation and spread of knowledge has been recognised as a legitimate concern of the State.

⁴⁵⁶ Article 19(1)(a), Constitution of India.

⁴⁵⁷ A. D. Baets, A Historian's View on the Right to be Forgotten, 30 International Review of Law, Computers and Technology (2016) at pp. 57-66.

⁴⁵⁸ For instance, see M. Mostert et al., Big Data In Medical Research And Eu Data Protection Law: Challenges to the Consent or Anonymise Approach, 24(7) Journal of Human Genetics (2016); J. Tu et al., Impracticability of Informed Consent in the Registry of the Canadian Stroke Network, 350(14) New England Journal of Medicine (2004) at pp. 1414–1422.

⁴⁵⁹ See Valerie Steeves, Data Protection and the Promotion of Health Research, 2(3) Healthcare Policy (2007) at pp. 26-38.

⁴⁶⁰ Examples include South Africa (Section 27(1)(d), POPI Act), EU (Article 5(1) and Article 89, EU GDPR) and the UK (Section, 33 DPA).

⁴⁶¹ Recital 158, EU GDPR.

health.⁴⁶² Historical research, while not explicitly defined is understood to include research for genealogical purposes.⁴⁶³ Statistical research means any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results with these results capable of being used for different purposes including scientific purposes.⁴⁶⁴

The underlying theme across these categories and the manner in which they have been defined is the advancement of knowledge in public interest. Our law would extend the exemption to research, archival and statistical purposes due to this aspect inherent in each of these activities, since the meaning of the term research is well understood.

(c) Application of Obligations

The research exemption is not being envisaged as a blanket exemption. Only those obligations should be exempted where it is necessary to achieve the object of the research in public interest. Cases in which obligations may have to be exempted are however contextual and dependent on the nature of the research. Thus for instance, while consent and notice requirements may be a *sine qua non* in most forms of medical research such as clinical trials, requirements of informed and opt-in consent may be not be appropriate models for large scale population health research where non-participation may introduce bias thereby influencing the accuracy of the results.⁴⁶⁵ Even research processing that is not intended to identify particular persons would be hit by the law if the research data contains enough features to inadvertently allow for such identification.

Purpose specification, which requires the data fiduciary to process for a specific purpose that must be known at the time of collection, may similarly not apply in cases where overwhelming amounts of data. While not collected for research purposes, these may possess the potential to gain research value afterwards.⁴⁶⁶ Similarly data storage obligations that require data to be retained as long as retention is necessary to achieve the purpose of processing may not apply since it can inhibit potential research opportunities. It is difficult to always predict the various ways in which a dataset can be used by researchers in the future.⁴⁶⁷

Data principal rights such as access, confirmation and correction may sometimes prove to be onerous to comply with by research organisations processing such data since they may not have the resources to ensure effective compliance. Moreover, exercise of rights such as right

⁴⁶² Recital 159, EU GDPR.

⁴⁶³ Recital 160, EU GDPR.

⁴⁶⁴ Recital 162, EU GDPR.

⁴⁶⁵ See Chapter 64: Research, Australian Privacy Law and Practice (ALRC Report 108).

⁴⁶⁶ A. D. Baets, A historian's view on the right to be forgotten, Vol. 30 International Review of Law, Computers and Technology (2016).

⁴⁶⁷ Ateneo De Manila University, Philippines, Is Research Exempt From Data Protection? available at <https://www.ateneo.edu/udpo/article/Is_research_exempt_from_data_protection> (last accessed on 2 May 2018).

to be forgotten may prove inherently detrimental to historical research or other research based on longitudinal data.⁴⁶⁸

However, since the exemption of obligations will be highly context specific it is difficult to lay down a bright line test that exhaustively provides for which obligations will be exempted in what circumstances. In fact, laying down requirements in the law may result in too broad an exemption for categories such as sensitive medical research where standards like consent should otherwise be the norm.⁴⁶⁹ Hence, the DPA will have the authority to exempt the operation of obligations if they effectively preclude the achievement of the research purpose. Further, the DPA may also exempt the operations of obligations if compliance will disproportionately divert resources from the achievement of the research purpose.

Safeguards with regard to processing for research purposes are however essential to ensure that the research exemption is not misused. Processing under the exemption would thus be conditional on the processing of data not supporting decisions with respect to individuals⁴⁷⁰ or the processing creating a risk of significant harm to individuals. The operation of the various exemptions for research purpose would therefore be subject to these conditions at all times. Further, measures such as de-identification should also be undertaken where the research can still be carried out under such conditions. It is also necessary to ensure that data is not processed in a manner that supports targeted actions with regard to individuals. Obligations such as data security that require the implementation of technical and organisational measures to ensure the confidentiality, integrity and accessibility of data will continue to apply. Lastly, any applicable codes of ethics with regard to processing of special categories of research such as medical research will in any case have to be complied with at all times.

V. Personal or Domestic Purposes

(a) Context

Processing activities of an individual which are insignificant and are carried out for a purely personal or domestic purpose are usually placed outside the scope of a data protection law. This is because such processing is considered necessary for the development of the individual and cultivation of social relationships. For instance, where an individual has used a camera to take photographs and record videos of surroundings while on vacation, even though this would include personal data of persons captured on camera, the personal exemption would apply as it relates to an individual's personal activity for the cultivation of social relationships and role as a member of society. For these reasons, data protection laws across jurisdictions

⁴⁶⁸ Ateneo De Manila University, Philippines, Is Research Exempt From Data Protection? available at <https://www.ateneo.edu/udpo/article/Is_research_exempt_from_data_protection> (last accessed on 2 May 2018).

⁴⁶⁹ The broad nature of research exemption under the EU GDPR has in fact been criticised as being detrimental to the interests of individuals especially in the context of genetic research, see K. Pormeister, Genetic Data and the Research Exemption: Is The GDPR Going Too Far?, 7(2) International Data Privacy Law (2017).

⁴⁷⁰ Such conditions have been imposed by Section 33, UK DPA in the context of the research exemption.

have had little involvement with private citizens processing their personal data for a domestic purpose.⁴⁷¹

The key question that arises in this context is what is meant by ‘personal’. As per the Court of Justice of the EU’s decision in *Bodil Lindqvist*,⁴⁷² if personal data disseminated on the internet is accessible to an indefinite number of people, then such dissemination would not qualify as personal or domestic processing as the purpose ceases to remain ‘purely personal’.

Further, several data protection legislation exempt personal data processed by natural persons “in the course of a purely personal or household activity”.⁴⁷³ An implicit distinction has been drawn between purely personal activity having no professional or commercial nexus, and personal activity bearing such nexus. For example, personal views about friends expressed on a private social media account would be exempt under this provision, as it is a purely personal activity. However, views expressed on a public social media profile by employees of an organisation may not be exempt. This is because there is a commercial nexus to the activity as it is in the context of the activities of a commercial venture.

As the scope of activities that may be considered ‘personal’ widens, the possibility of conflating the personal or domestic exemption with other exemptions may increase. For example, an individual’s personal blog may qualify for both the personal and journalistic exemptions, depending on the nature of the content, the frequency and scale at which the content is disseminated, the nature of the blog etc.

The widespread use of social networking services leads to a similar conflation.⁴⁷⁴ Access to the internet has enabled individuals to disseminate information quickly and widely, an ability formerly restricted to media and publishing organisations.⁴⁷⁵ Users exercise control over the information that they disclose online, which often contains personal data related to them. In some cases, information shared by such individuals may also include personal data related to

⁴⁷¹ Proposals for Amendments regarding exemption for personal or household activities available at <http://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf> (last accessed on 12 April 2018).

⁴⁷² *Lindqvist v Åklagarkammaren i Jönköping*, Case C-101/01.

⁴⁷³ Article 2(2)(c), EU GDPR; Section 36, UK DPA; Art. 2(2)(a); Section 5(3), Personal Data Protection Code, 2003, Italy. See also Recital 18, EU GDPR provides: “this Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.”

⁴⁷⁴ Rebecca Wong, Social Networking: a Conceptual Analysis of a Data Controller, 14(5) Communications Law (2009).

⁴⁷⁵ Rebecca Wong, Social Networking: a Conceptual Analysis of a Data Controller, 14(5) Communications Law (2009). See also Article 29 Working Party, Opinion on Data Protection Issues Related to Search Engines, available at <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf> (2008); UK Information Commissioner’s Office, Social networking and online forums- when does the DPA apply? available at <<https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2013/06/UK-ICOsocial-networking-and-online-forums-dpa-guidance.pdf>> (last accessed on 3 May 2018).

their friends and family, or other individuals (for example, tagging strangers or third parties in photographs without their consent). Such disclosure may be made to a restricted friend list or to the public at large. In such cases, the application of the personal/domestic exemption would depend on the nature of the post. For instance, as per the principles laid down in *Lindqvist*,⁴⁷⁶ even a private social media post containing personal data of individuals other than the user may not be covered by the personal exemption depending on the facts of the case. The individual here would be a data fiduciary.

Similarly, a domestic CCTV installed in an individual's residential premises which captures the video of strangers cannot be regarded as strictly personal. In *František Ryneš*,⁴⁷⁷ the Court of Justice of the EU held that the image of a person recorded by a camera qualifies as personal data. The Court opined that a security camera system installed by an individual in her home which simultaneously monitors a public space does not qualify as purely personal or domestic activity.

(b) Scope

The Committee recognises that activities carried out by individuals for a private purpose, or in fulfilment of a daily domestic task requires protection. Therefore, a narrowly tailored exemption for purely personal or domestic processing of data should be incorporated in the data protection law. If an act of processing falls within this category, the obligations and rights under the law will not apply as such application would be disproportionate, impracticable and onerous on the individual. In other words, processing of both personal and sensitive personal data carried out for a personal or domestic purpose would enjoy a blanket exemption from the application of the data protection law.

(c) Application of Obligations

The Committee acknowledges that the absolute nature of this exemption means that the determination of whether an activity is purely personal or domestic will be paramount. Therefore, an activity would not be considered purely personal or domestic if such processing involves any public disclosure, or if it involves any professional or commercial activity. The exemption would not apply in these cases. In the EU, certain guidelines have been laid down to ascertain whether an act of processing is personal, such as the number of people the personal data is being disseminated to, whether the personal data is about individuals who are not personally related to the individual posting it, scale and frequency of processing, potential harm, and whether it is partly personal and partly professional.⁴⁷⁸ If processing falls outside

⁴⁷⁶ Lindqvist v Åklagarkammaren i Jönköping, Case C-101/01

⁴⁷⁷ František Ryneš v. Úřad pro ochranu osobních údajů, Case C212/13, 11 December 2014; See also Lindqvist v. Åklagarkammaren i Jönköping, Case C-101/01.

⁴⁷⁸ Proposals for Amendments regarding exemption for personal or household activities available at <http://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf> (last accessed on 12 April 2018); Lindqvist v Åklagarkammaren i Jönköping, Case C-101/01.

of this ambit, the data protection law will continue to apply.⁴⁷⁹ Similar guidelines may evolve in the Indian context through case laws over the course of time. This provision would ensure that the law does not become onerous for private individuals, as well as prevent misuse by individuals for professional or commercial gains.

VI. Journalistic Activities

(a) Context

(i) Conflict between Privacy and Free Speech

A good data protection law needs to achieve a balance between competing social interests. One such conflict exists between the right to free flow of information through freedom of speech and expression and the right to restrict such flow in the interest of privacy and safeguarding of the handling of personal data.

Freedom of expression is necessary to ensure a participatory democracy where citizens have free and fair access to information. Given the large volume of information and the multiple sources such information originates from, journalists and media houses act as the conduit to relay such information in an accessible manner. The role of a journalist is to be ‘an analyst and interpreter of the events’⁴⁸⁰ and to serve as ‘proxy witnesses and information-gatherers’.⁴⁸¹ Journalism acts in public benefit since it helps in building social accountability and brings about discussions on issues of public concern.⁴⁸² If journalists were made to adhere to the grounds of processing personal data, it would be extremely onerous for them to access information. Further, mandating grounds of processing like consent would mean that accounts that are unfavourable to the data principal would simply not get published. There therefore exists a public interest in the untrammelled dissemination of news, current affairs and documentaries, especially when they inform, criticise and analyse issues of public importance. However, it could be argued that even material apart from the above may be relevant to the general interests of the public and the flow of such information should not be impeded.

⁴⁷⁹ See *The Law Society and Others v. Rick Kordowski (Solicitors from Hell)*, [2011] EWHC 3185 (QB) where the individual was held to be a data controller.

⁴⁸⁰ Donald H. Johnston, *Journalism and the Media* (1979) at p. 108 as cited in Jonathan Peters and Edson C. Tandoc, Jr., *People Who Aren’t Really Reporters At All, Who Have No Professional Qualifications: Defining a Journalist and Deciding Who May Claim the Privileges*, *New York University Journal of Legislation and Public Policy* (2013).

⁴⁸¹ Judith Clarke, *How Journalists Judge the ‘Reality’ of an International ‘Pseudo-Event’*, 4 *Journalism* (2003) as cited in Jonathan Peters and Edson C. Tandoc, Jr., *People Who Aren’t Really Reporters At All, Who Have No Professional Qualifications: Defining a Journalist and Deciding Who May Claim the Privileges*, *New York University Journal of Legislation and Public Policy* (2013).

⁴⁸² William F. Woo, *Defining a Journalist’s Function*, 59 *Nieman Reps* (2005) at p. 33 as cited in Jonathan Peters and Edson C. Tandoc, Jr., *People Who Aren’t Really Reporters At All, Who Have No Professional Qualifications: Defining a Journalist and Deciding Who May Claim the Privileges*, *New York University Journal of Legislation and Public Policy* (2013).

At the same time, as has been stressed throughout this report, the fundamental right to privacy encompasses within itself the protection of personal data of individuals and therefore, needs protection. The Supreme Court of India, in the case of *R. Rajagopal v. State of Tamil Nadu*⁴⁸³ has held that citizens have the right to protect their privacy and the publication of personal information without consent regardless of the nature of content of such publication may violate the privacy of the person concerned.

To be able to give effect to both these rights, it is essential to ensure a balance between the freedom of expression and the safeguarding of personal data for the public good of a free and fair digital economy. This can be done by allowing recourse to the journalistic exemption where public interest in the disclosure of the personal data is overriding. Here it becomes important to determine what public interest means. The standard for determining whether the published material violates the concerned individual's privacy would be that of a reasonable person and not that of a hyper sensitive person.⁴⁸⁴ It has also been held that public interest has to be more than mere idle curiosity. The balance between freedom of expression and privacy has to be struck by considering factors such as the interest of the community and the proportionality of protecting one right against the infraction of the other.⁴⁸⁵ In the US, a standard of newsworthiness is used instead where the term would include material which could be 'fairly considered as relating to any matter of political, social, or other concern to the community' or when it 'is a subject of general interest and of value and concern to the public.'⁴⁸⁶ The threshold for what counts as public interest is understandably low and vague,⁴⁸⁷ although, the Indian judiciary has laid down factors like likelihood of injustice, sensitivity of the relevant information, passage of time and class of persons affected to broadly draw out a scope for the term.⁴⁸⁸

To be able to strike a balance between the aforementioned rights and be able to ascertain when one right should constrain the other, it is important to first be guided by what would best serve public interest. Second, the broad contours of what journalism and a journalist would signify should also be laid down. Finally, it is essential to ensure that journalists do not abuse the rights of the data principals by mandating that they are committed to upholding certain standards of privacy which are coterminous with the data protection law.

⁴⁸³ R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.

⁴⁸⁴ Ajay Goswami v. Union of India, (2007) 1 SCC 143.

⁴⁸⁵ Indu Jain v. Forbes Incorporated, (2007) ILR 8 Delhi 9.

⁴⁸⁶ Snyder v. Phelps, 562 U.S. 443 (2011).

⁴⁸⁷ Bihar Public Service Commission v. Saiyed Hussain Abbas Rizwi, (2012) 13 SCC 61 held "The expression "public interest", like "public purpose", is not capable of any precise definition. It does not have a rigid meaning, is elastic and takes its colour from the statute in which it occurs, the concept varying with time and state of society and its needs." The Black's Law Dictionary defines it as the general welfare of the public that warrants recognition and protection; something in which the public as a whole has a stake."

⁴⁸⁸ R.K. Jain v. Union of India, (1993) 4 SCC 120 held that "the factors to decide public interest would include, "(a) where the contents of the documents are relied upon, the interests affected by their disclosure; (b) where the class of documents is invoked, whether the public interest immunity for the class is said to protect; (c) the extent to which the interests referred to have become attenuated by the passage of time or the occurrence of intervening events since the matters contained in the documents themselves came into existence; (d) the seriousness of the issues in relation to which production is sought; (e) the likelihood that production of the documents will affect the outcome of the case; (f) the likelihood of injustice if the documents are not produced."

Journalism has been interpreted as ‘the process of gathering, selecting, interpreting, and disseminating news’.⁴⁸⁹ While news would ordinarily be the most common type of output of journalism, the definition of news itself may be vague. Further, it has also been argued that news would not be the only output of journalism. For example, opinions may be a relevant output of journalism.⁴⁹⁰ Thus the definition of journalism is continuously expanding, and adequate care must be taken to make it inclusive.⁴⁹¹

This also leads to the question of whether anyone who engages in journalism could be deemed a journalist and accorded the journalistic exemption or if there needs to exist a definition of journalist as well. Who a journalist could be, may be characterised by factors such as the medium of publication, the hierarchy she operates in, the activities she engaged in, the output she delivers, the social role of her work and the ethics followed by her.⁴⁹²

Recently citizen journalists have started to occupy a presence in the market for news given the ease of access to internet which allows citizens to publish in real time to a worldwide audience.⁴⁹³ Therefore, constraining the definition of a journalist to someone employed by a media organisation would exclude a sizeable proportion of people who disseminate news to the public. Thus, factors such as how often a person does activities for a journalistic purpose or whether they obtain their livelihood from carrying out activities for a journalistic purpose may be better suited in determining who a journalist is.

(ii) Ethics Standards

⁴⁸⁹ Donald H. Johnston, *Journalism and the Media* (1979) at p. 2-3 as cited in Jonathan Peters and Edson C. Tandoc Jr., *People Who Aren’t Really Reporters at All, Who Have No Professional Qualifications: Defining a Journalist and Deciding Who May Claim the Privileges*, *New York University Journal of Legislation and Public Policy* (2013).

⁴⁹⁰ Kimberly Meltzer, *The Hierarchy of Journalistic Cultural Authority: Journalists’ Perspectives According to News Medium*, 3 *Journalism Practice* (2009) at pp 59, 62 and 71–72 as cited in Jonathan Peters and Edson C. Tandoc Jr., *People Who Aren’t Really Reporters at All, Who Have No Professional Qualifications: Defining a Journalist and Deciding Who May Claim the Privileges*, *New York University Journal of Legislation and Public Policy* (2013).

⁴⁹¹ Guidance may be taken from other jurisdictions which have aimed to understand what journalistic activities entail. For example, in Australia ‘journalism’ has been understood as collection, preparation for dissemination or dissemination of material to make available to the public where such material is in the character of news, current affairs or a documentary, or an opinion or analysis of any of these, see Chapter 42: Journalism Exemption in Australian Law Reform Commission, *Australian Privacy Law and Practice* (ALRC Report 108); In the UK, the journalism exemption is constrained by conditions like the data should have been processed with a view to publish and that such publication should be in public interest and should not be incompatible with journalism, see Section 32, UK DPA.

⁴⁹² Jonathan Peters and Edson C. Tandoc Jr., *People Who Aren’t Really Reporters at All, Who Have No Professional Qualifications: Defining a Journalist and Deciding Who May Claim the Privileges*, *New York University Journal of Legislation and Public Policy* (2013).

⁴⁹³ Dan Gillmor, *We The Media: Grassroots Journalism By The People, For The People* (2006) as cited in Jonathan Peters and Edson C. Tandoc Jr., *People Who Aren’t Really Reporters at All, Who Have No Professional Qualifications: Defining a Journalist and Deciding Who May Claim the Privileges*, *New York University Journal of Legislation and Public Policy* (2013).

Finally, to be accorded an exemption from the data protection law, journalists should be bound by ethics standards like honesty and fairness in collecting and disseminating personal data for the purpose of news reporting. The purpose of having ethics standards in place for the application of the journalistic exemption is to be able to ‘separate credible contributors from less credible ones by establishing benchmarks of professional practice and measuring people against them’.⁴⁹⁴ Ethics standards have become especially important in the age of the internet which has made publishing infinitely easier, with the result that persons without the skills or training in becoming a journalist are becoming the source for news.⁴⁹⁵ The lack of any professional qualification examination further intensifies this problem.

To ensure accountability on the part of media houses engaging in journalism, the ALRC was of the opinion that all media houses should be publicly committed to observe published privacy standards which are considered adequate by the data protection regulatory authority.⁴⁹⁶ This is a proposal that deserves to be adhered to.

Further, News Broadcasters Association in its submission to the Committee outlined some ethics standards that journalists should adhere to: (i) facts that are published should be accurate, fair, neutral, objective, relevant and impartial; (ii) data should be kept securely; (iii) the publication should be with the aim of dissemination of information, opinions and ideas to the public; and (iv) personal data should be processed while considering the data principals’ right to privacy.⁴⁹⁷ Such ethics standards may be set by various regulatory organisations in the media, and journalists who adhere to these standards should be accorded the exemption under the data protection law. Independent journalists may self-certify through a declaration that they are adhering to the aforementioned ethics standards.

(b) Scope

As discussed above, to be able to strike a balance between freedom of expression and right to informational privacy, the data protection law would need to signal what the term ‘journalistic purposes’ signifies, and whether an activity for such purposes furthers public interest. From a careful review of public comments and jurisprudential guidance from India and other countries, this would mean that an activity for a journalistic purpose would necessarily have to be linked with an intention to publish or disseminate content, and for such publication or dissemination to occur in public interest.

⁴⁹⁴ Erik Ugland and Jennifer Henderson, Who Is a Journalist and Why Does It Matter? Disentangling the Legal and Ethical Arguments, 22 *Journal of Mass Media Ethics* (2007) at p. 243 as cited in Jonathan Peters and Edson C. Tandoc Jr., People Who Aren’t Really Reporters at All, Who Have No Professional Qualifications: Defining a Journalist and Deciding Who May Claim the Privileges, *New York University Journal of Legislation and Public Policy* (2013).

⁴⁹⁵ Alan Knight, Who is a Journalist? 9 *Journalism Studies* (2008) at p. 117 as cited in Jonathan Peters and Edson C. Tandoc Jr., People Who Aren’t Really Reporters at All, Who Have No Professional Qualifications: Defining a Journalist and Deciding Who May Claim the Privileges, *New York University Journal of Legislation and Public Policy* (2013).

⁴⁹⁶ See Chapter 42: Journalism Exemption, Australian Privacy Law and Practice (ALRC Report 108).

⁴⁹⁷ Comments in response to the White Paper submitted by News Broadcasters Association on 31 January 2018, available on file with the Committee.

To infuse a measure of accountability, persons or entities being granted this exemption should be bound to follow ethical standards which sufficiently protect the privacy of data principals which are set out by various regulatory organisations in the media. A public commitment of this nature should be made mandatory.

This would apply to the processing of both personal and sensitive personal data.

(c) Application of Obligations

The standards of specificity as ordinarily required under purpose limitation should not apply in case of journalistic exemption since it is often exploratory in nature and it would be impractical to expect a journalist to specify in exact terms the purposes the personal data is being collected for. Purpose limitation will not apply, though to the extent possible, journalists should still be expected to outline the broad contours of the purpose for which the personal data is being collected, with the final purpose being the publishing of news on the subject. Further, personal data processed for the purpose of journalism should ordinarily be deleted when the purpose of such processing has been realised, that is, when the news has been published.

However, to cover new stories journalists may often need to reach for past records of data and the deletion of personal data collected post publishing may make it very difficult to do so. Therefore, under the journalistic exemption storage limitation should not apply so long as it is clear that the personal data is being stored for only for further journalistic purposes. The notice and consent obligation will not apply, especially in cases of investigative journalism where notifying the individual of the collection of information about them would defeat the purpose of the exercise. However, the journalist undertaking such an activity must have a clear reason (usually public interest) which outweighs the violation of privacy. Such an assessment would usually include the importance of the news, the possibility of verification of information, the level of intrusion into the data principal's privacy and the potential impact upon the data principal and third parties.

While codes such as those issued by the Press Council of India stress the importance of privacy, there is a need for more detailed guidance on specific obligations of the nature discussed above. For instance, while the Norms of Journalistic Conduct laid down by the Press Council of India state that in certain situations, consent of the data principal ought to be taken, the list is not comprehensive and does not lay down the consequences of not following these norms.⁴⁹⁸ Similarly, the Code of Ethics and Broadcasting Standards released by the National Broadcasting Authority only states that privacy must be respected unless there is a 'clearly established larger and identifiable public interest' without elaborating on factors which would lead to the identification of such public interest. The Codes also do not lay

⁴⁹⁸ Press Council of India, Norms of Journalistic Conduct (2010) available at <<http://presscouncil.nic.in/OldWebsite/NORMS-2010.pdf>> (last accessed on 2 May 2018).

down obligations relating to how long personal data collected during the course of journalism can be retained for, or how it is to be secured, or data principals' rights in such data.⁴⁹⁹ It is expected that such matters will be dealt with in codes of ethics that bind journalists obviating the need for the data protection law to impose such obligations on journalists. Therefore, the codes as they exist now will need to be revised to ensure that they act as a sufficient measure of accountability such that the application of journalistic exemption does not lead to undue violation of the data protection rights of data principals.

Security safeguards should be implemented for all personal data processed by journalists. Therefore, they must take reasonable steps to prevent the data's loss, theft or misuse. Those who avail of the exemption should ensure that their published work is not misleading and distinguishes facts from opinions, apart from adhering with ethics standards.

Requests to implement data principal rights like right to access, confirm and correct can be refused by those taking cover of the journalistic exemption because complying with such requests would often be incompatible with journalism. Such requests may be rejected both before and after publication. A request made before publication could be refused since the provision of such information may lead to attempts to block publication or gathering of further information. An exemption from this obligation may also be necessary to stop persons from harassing journalists by inundating them with requests with a view of blocking or slowing down investigation or publishing of a piece of news. The financial and human resource implications of compliance with such requests may also frustrate journalistic activity, especially for independent journalists.

It should be borne in mind that the exemptions from obligations would only apply so long as the personal data is being processed for journalistic purposes and in a fair and reasonable manner. Thus, the basic obligation of fair and reasonable processing would continue to apply, shaped by this context.

VII. Manual Processing by Small Entities

(a) Context

The obligations placed on data fiduciaries as a part of data protection law are largely aimed at ensuring that data principals are not subjected to privacy harms and the obligations placed on fiduciaries are thus designed to mitigate and prevent the harms caused by risky practices arising out of electronic data processing using automated means. Such technologies substantially increase the risk of harm from personal data processing due to the added ease of recording, dissemination, viewing and systematic analysis.⁵⁰⁰ An important question that arises is whether all the obligations imposed on entities carrying out such processing need to be imposed on other entities processing by means other than automated ones. While there is a

⁴⁹⁹ News Broadcasters Association, New Delhi, Code of Ethics & Broadcasting Standards (2008) available at <http://www.nbanewdelhi.com/assets/uploads/pdf/code_of_ethics_english.pdf> (last accessed on 3 May 2018).

⁵⁰⁰ Jerry Kang, Information Privacy in Cyberspace Transactions, 50 Stanford Law Review (1998) at p.1198.

risk that such fiduciaries may create privacy harms, the Committee is of the view that they may not need to be subjected to the same legal duties.

(b) Scope

While it may be necessary to ensure that entities carrying out manual processing are subjected to data protection law, it is also important to ensure that any exemption from burdensome obligations that has been designed specifically for them does not become a loophole through which organisations execute their most harmful activities. For instance, the small business exemption in Australia⁵⁰¹ is criticized as being too broad, allowing for large swathes of processing activities to go unchecked.⁵⁰² Any such exemption should thus only be held out to those entities that would relatively have to bear the heaviest burdens from data protection obligations despite carrying out activities that only raise limited privacy risks. A turnover-based exemption appears to cover those entities that would suffer the most from legal obligations and such a scheme may be seen in some legal regimes.⁵⁰³ However, this may not make for an appropriate classification as many entities with little or no turnover may nonetheless be processing large volumes of personal data and may, therefore, give rise to substantial harm. The Committee is thus of the view that apart from a turnover-based condition, to avail of this exemption an entity should not process personal data of data principals exceeding a specified number calculated over a definite time period. It must also not collect personal data for the purpose of disclosing it to other parties. In this manner, the exemption may be restricted to small entities processing a limited amount of personal data manually without any intention of further disclosure.

(c) Application of Obligations

The obligations from which the entity is to be exempted must similarly be restricted to the most burdensome or costly ones, without limiting the essential protections that data protection law otherwise offers. Obligations that may be onerous in this context are notice, data quality, storage limitation, certain aspects of the right to access, the right to portability, and the right to be forgotten (which is largely inapplicable in this case), apart from organizational measures related to privacy by design, transparency and security safeguards. These leave in place core obligations regarding purpose and collection limitation as well as data principal rights such as confirmation, access and correction.

⁵⁰¹ See Section 6D of the Privacy Act, 1988 (pegging the threshold for the annual turnover of a ‘small business operator’ at \$3 million, apart from placing other conditions).

⁵⁰² See, comments in response to the White Paper submitted by Graham Greenleaf on 31 January 2018, available on file with the Committee, at p. 8 (remarking that Australia may be the only country with such a small business exemption with its application extending to 94% of all businesses).

⁵⁰³ Such exemptions exist in India, for example, for the merger control regime under the Competition Act, 2002 (see, Ministry of Corporate Affairs, Government of India, Notification regarding Target Exemption available at <<http://www.cci.gov.in/sites/default/files/notification/SO%20673%28E%29-674%28E%29-675%28E%29.pdf>> (last accessed on 26 May 2018)), and for licensing requirements under the Food Safety and Standards Act, 2006 (see, Regulation 1.2.1(4), Food Safety and Standards (Licensing and Registration of Food Business) Regulations, 2011).

RECOMMENDATIONS

Non-Consensual Grounds of Processing

- **Functions of the State:** Welfare functions of the state will be recognised as a separate ground for processing. Processing activities carried out by the State under law will be covered under this ground, ensuring that it is in furtherance of public interest and governance. However, only bodies covered under Article 12 of the Constitution may rely on this ground. Processing towards activities that may not be considered part of a welfare functions would, however, not to be permitted. Thus, the availability of this ground is restricted to certain entities and certain functions to avoid vagueness in the law. **[Sections 13 and 19 of the Bill]**
- **Compliance with Law or Order of Court or Tribunal:** Compliance with law or order of court or tribunal will be recognised as a separate ground for processing to avoid inconsistency with obligations under other laws, regulations and judicial orders. The word ‘law’ shall be construed to mean laws, ordinances, orders, bye-law, rules, regulations and notifications that have statutory authority. Order of court or tribunal would be restricted to Indian courts and tribunals. Obligations imposed by contract, foreign law and foreign judicial orders shall not be permitted to be processed under this ground. **[Sections 14 and 20 of the Bill]**
- **Prompt Action:** Prompt action will be recognised as a separate ground for processing. It should receive a strict interpretation and only be applied in critical situations where the individual is incapable of providing consent and the processing is necessary to meet emergency situations. **[Sections 15 and 21 of the Bill]**
- **Employment:** Employment will be recognised as a separate ground for processing. This ground should be invoked only where processing under consent would involve disproportionate effort or where the employment relation makes consent inappropriate and will permit processing even where employment-related activities are not authorised under any of the other grounds of processing such as compliance with law. **[Section 16 of the Bill]**
- **Reasonable Purpose:** Reasonable purpose is a residuary ground for processing activities which are not covered by other grounds like consent, compliance with law, prompt action and public function but are still useful to society. The ambit of the provision would be limited to those purposes which are whitelisted by the DPA to guide data fiduciaries. **[Section 17 of the Bill]**

Exemptions

- Security of the State: The data protection law will enable an exemption to the processing of personal or sensitive personal data if it is necessary in the interest of the security of the state. Any restriction must be proportionate and narrowly tailored to the stated purpose. The Central Government should expeditiously bring in a law for the oversight of intelligence gathering activities. [Section 42 of the Bill]
- Prevention, Detection, Investigation and Prosecution of Contraventions of Law: The data protection law should provide an exemption for prevention, detection, investigation and prosecution of contraventions of law (including protection of revenue). In order to invoke the exemption, the law enforcement agencies must be authorised by law. [Section 43 of the Bill]
- Disclosure for the Purpose of Legal Proceedings: The disclosure of personal data necessary for enforcing a legal right or claim, for seeking any relief, defending any charge, opposing any claim or for obtaining legal advice from an advocate in an impending legal proceeding would be exempt from the application of the data protection law. General obligations of security and fair and reasonable processing will continue to apply. [Section 44 of the Bill]
- Research Activities: The research exemption is not envisaged as a blanket exemption. Only those obligations that are necessary to achieve the object of the research will be exempted by the DPA. This assessment is contextual and dependent on the nature of the research. [Section 45 of the Bill]
- Personal or Domestic Purposes: A narrowly tailored exemption for purely personal or domestic processing of data should be incorporated in the data protection law. It would provide a blanket exemption from the application of the data protection law. [Section 46 of the Bill]
- Journalistic Activities: To strike a balance between freedom of expression and right to informational privacy, the data protection law would need to signal what the term ‘journalistic purposes’ signifies, and how ethical standards for such activities would need to be set. Where these conditions are met, an exemption should be provided. [Section 47 of the Bill]
- Manual Processing by Small Entities: Since the risk of privacy harms being caused are higher when personal data is processed through automated means, an exemption will be made in the data protection law for manual processing by data fiduciaries that are unlikely to cause significant harm and would suffer the heaviest relative burdens from certain obligations under this law. [Section 48 of the Bill]

CHAPTER 9: ENFORCEMENT

Ultimately, any law is only as good as its enforcement. To ensure that India enjoys a robust data protection regime which ensures that its substantive obligations are respected, a competent enforcement mechanism is of the utmost importance. This chapter sets out the means by which accountability for obligations on entities is ensured in a fair and effective manner.

Based on a review of the theoretical literature, practical experience of other countries in enforcing data protection laws, the experience of our own country with respect to enforcement and public comments to our White Paper, a responsive regulatory framework equipped with a range of tools has been found by us to be of critical importance.⁵⁰⁴ Enforcement should, where possible, be front-ended, i.e. require *ex ante* compliance by entities with substantive obligations under the law. Where determination of liability for violations is required, a well-resourced DPA, with necessary powers is required to be set up. Given the scale of enforcement, such DPA must work closely with sectoral regulators and self-regulatory or industry bodies, both to formulate codes of practice relating to several issues of data protection as well as to prevent any regulatory overlap in determining liability.

This chapter sets out the aforementioned framework in three sections: first, the structure and functions of the regulator (the DPA) and the tools that will be used for regulation; second, the classification of and obligations on certain data fiduciaries that will be regulated; and third, the remedies available in case of violations of the provisions set out under the data protection law.

In making recommendations on the issues arising in relation to enforcement of a data protection law, the Committee has relied on several helpful public submissions made to the White Paper, particularly those by Dvara Research⁵⁰⁵ and NIPFP *et al.*⁵⁰⁶

A. The Data Protection Authority: Structure, Functions and Tools

I. White Paper and Public Comments

After conducting a preliminary study of other jurisdictions, the White Paper suggested the creation of an independent regulatory body for enforcement of a data protection legal framework. Further, it was suggested that this regulatory body should have the powers of (a) monitoring, enforcement and investigation; (b) awareness generation; and (c) standard setting. It was suggested that a number of regulatory tools and mechanisms such as codes of

⁵⁰⁴ Graham Greenleaf, Asian Data Privacy Laws: Trade and Human Rights Perspective (Oxford University Press, 2014).

⁵⁰⁵ Comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee.

⁵⁰⁶ Comments in response to the White Paper submitted by the National Institute of Public Finance and Policy, Mozilla Foundation and Vrinda Bhandari, available on file with the Committee.

practice and categorisation of data fiduciaries could be deployed to achieve enforcement objectives.⁵⁰⁷

Most commenters were of the view that a separate, independent authority needs to be constituted to carry out general functions related to data protection. Favoured measures for maintaining the independence of the body include fixed tenure, disclosure of conflicts, post-retirement safeguards and restrictions on future employment, and financial independence. Various commenters suggested that the functions of the DPA should involve investigation, registration, standard-setting and adequacy assessments. The recommended composition includes a chairperson and members with technical and legal expertise. They should be appointed by a committee composed of members from the judiciary, the executive, civil society, and industry representatives. In addition, some commenters opined that state level authorities may be necessary in sharing the considerable regulatory burden; while others argued that allowing state authorities would result in an increase in costs, threat of double prosecution, and inconsistency in the applicable legal position.

Most commenters were of the view that an individual whose data protection rights have been violated may first approach the grievance redressal officer of the data fiduciary. Where the data fiduciary fails to resolve the complaint of the individual in a satisfactory or expeditious manner, the data principal may approach the DPA for recourse. The DPA may also initiate action against a data fiduciary on a *suo motu* basis. Qualifications of the adjudicating officer, as suggested by the commenters, include a graduate degree or its equivalent, and specific expertise in law and information technology. The commenters were in agreement that the adjudicating officer should have the powers of a civil court and be able grant compensation as well as impose monetary penalties. Most commenters were of the view that an appeal from the order of the adjudicating officer may lie with a specialised data protection appellate tribunal. These views have been fully considered while laying out the enforcement structure below.

II. Analysis

(a) Structure and Functions of the DPA

(i) Establishment

The DPA shall be in the nature of a high-powered, independent national body in view of the significance of creating an ecosystem of responsible data handling. The DPA, a sector-agnostic body, will ensure that every entity that handles data is conscious of its obligations and that it will be held to account in case of failure to comply. The DPA shall be a body corporate having perpetual succession and a common seal with the power to acquire, hold or dispose of property. Further, it will have the capacity to contract and to sue or be sued. It

⁵⁰⁷ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at Part IV, Chapter 2.

shall be a single institution with appropriate regional offices in order to fulfil its various statutory functions.⁵⁰⁸

(ii) Composition

It is important to create a system for selecting members of the DPA in a fair and transparent manner, especially because it is expected that government agencies will be regulated as data fiduciaries under the data protection law. The DPA will be governed by a board consisting of six whole-time members and a chairperson appointed by the Central Government on the recommendation of a selection committee. The selection committee shall consist of the Chief Justice of India or her nominee (who is a judge of the Supreme Court of India), the Cabinet Secretary, Government of India, and one expert of repute who has special knowledge of, and professional experience in areas related to data protection, information technology, data management, data science, cyber and internet laws and related subjects.⁵⁰⁹

The members of the DPA should be individuals of integrity and ability with special knowledge of, and professional experience of not less than 10 years in, areas related to data protection, information technology, data management, data science, cyber and internet laws and related subjects.⁵¹⁰ Following this mechanism for selection and appointment is aimed at ensuring independence, expertise and non-partisanship in selecting members of the DPA.⁵¹¹

To ensure the independence of the members of the DPA, their employment shall be fixed for a term of five years subject to a suitable retirement age.⁵¹² The salaries and allowances should be prescribed by the Central Government. However, the terms and conditions of appointment of such members should not be changed to their disadvantage during their tenure. Furthermore, the members of the DPA shall not be permitted to accept employment either under the Central or State Governments, or under a significant data fiduciary, during the course of their tenure or for a period of two years thereafter.

(iii) Functions of the DPA

Broadly, the DPA may have four departments that shall perform the following functions: (1) monitoring and enforcement; (2) legal affairs, policy and standard setting; (3) research and

⁵⁰⁸ Section 3, SEBI Act. The SEBI Act has a similar provision establishing SEBI.

⁵⁰⁹ See similar provisions in Section 9, Competition Act; Sections 4(4), SEBI Act; Section 4, TRAI Act; Section 3, IRDA Act.

⁵¹⁰ See similar provisions in Section 8, Competition Act; Section 4(5), SEBI Act; Section 4, TRAI Act; Section 4, IRDA Act. . Inputs regarding qualifications of members of the DPA are adopted from Comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee.

⁵¹¹ Report of the Financial Sector Legislative Reforms Commission, Volume 1: Analysis and Recommendations (2013).

⁵¹² See similar positions in Section 10, Competition Act; Section 5, SEBI Act; Section 5, IRDA Act; and Section 5, TRAI Act.

awareness; and (4) inquiries, grievance handling and adjudication.⁵¹³ We have set out key particulars of each broad category below:

Monitoring and Enforcement

- (i) Monitoring and ensuring compliance, with the provisions of the data protection law;
- (ii) Issuance, renewal and revocation of registration certificates to data auditors and issuing a code of conduct for such auditors;
- (iii) Registration of significant data fiduciaries;
- (iv) Processing data breach notifications and taking action accordingly;
- (v) Assessing data audits;
- (vi) Monitoring cross-border transfer of personal data;
- (vii) Specifying circumstances where a DPIA may be required;
- (viii) Maintaining a database containing names of significant data fiduciaries and their rating in the form of data trust scores indicating compliance with obligations under the data protection law; and
- (ix) Specifying any other fee or charges, where relevant.

Legal Affairs, Policy and Standard Setting

- (i) Whitelisting activities processed under the ground of reasonable purpose;
- (ii) Making recommendations to the Central Government for green-lighting countries for cross-border transfer of personal data;
- (iii) Specifying residuary categories of sensitive personal data;
- (iv) Issuance of codes of practice;
- (v) Advising Parliament, Central Government, State Government and any regulatory or statutory authority on measures that must be undertaken to promote protection of personal data in accordance with the provisions of the data protection law;
- (vi) Advising the Central Government on acceding to any international instrument relating to data protection; and
- (vii) Issuing any guidance documents that may be necessary for the interpretation or suitable implementation of this law.

Research and Awareness

- (i) Generating awareness amongst data principals on their rights and the means to exercise them;⁵¹⁴

⁵¹³ The structure and functions of the DPA have been adopted from the comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee.

⁵¹⁴ Beni Chugh *et al*, Dvara Research Working Paper Series No. WP-2018-01 (July 2018) available at <<https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf>> (last accessed on 24 July 2018) at p.16.

- (ii) Promoting public awareness in understanding the risks, rules, safeguards and rights with respect to data protection including issuance of any public statement setting out trends in or specific instances of contravention of the provisions of the law;
- (iii) Educating data fiduciaries regarding data protection best practices and their obligations under the law;
- (iv) Monitoring technological developments and commercial practices which may affect data protection practices;⁵¹⁵ and
- (v) Promoting measures and undertaking research for innovation in the field of data protection.⁵¹⁶

The Committee finds it appropriate to point out that data protection law, even after the enactment of a general statute as proposed in this report, would still be in a nascent stage in India. The institutional structures and bodies of knowledge supporting the privacy of Indians would not develop unsupported in the course of the implementation of the law. It is thus imperative that a dedicated research wing be put into place within the structure of the DPA and that such wing work closely with the policy-making departments of the DPA to ensure the quality and effectiveness of its work.⁵¹⁷ This may extend into research regarding technical aspects of data protection, forensic data analysis practices, detection of uncharacteristic and unusual processing, algorithmic impact assessments, international practices as well as transnational flows of data, and other unique aspects of informational policy.

Inquiries, Grievance Handling and Adjudication

- (i) Calling for information, and undertaking inspections or inquiries into the affairs of data fiduciaries in accordance with the law;
- (ii) Delivering efficient, well informed, proportionate and timely enforcement actions;⁵¹⁸ and
- (iii) Interfacing with the data principal for handling complaints.⁵¹⁹
- (iv) Separate adjudication wing for adjudicating disputes (discussed below).

⁵¹⁵ For example, in the current technological scenario, the DPA should focus on the development of Internet of Things, AI and Big Data.

⁵¹⁶ For example, this research can take the form of a peer reviewed journal, thought leadership in the form of original articles and reports, establishment of doctoral chairs etc.

⁵¹⁷ Beni Chugh *et al*, Dvara Research Working Paper Series No. WP-2018-01 (July 2018) available at <<https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf>> (last accessed on 24 July 2018) at p.16.

⁵¹⁸ Adopted from the comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee. Such measures may include issuing a warning or a reprimand, requiring the data fiduciary to cease from taking a specific action, etc.

⁵¹⁹ This wing shall create an efficient infrastructure to receive and monitor the complaints of data principals. Complaints should be accepted via email, online portal, telephone, letter or in-person. Further, with changing technology, additional means of lodging complaints should be adopted.

(b) Enforcement Tools

Under the model of responsive regulation, it has been suggested that the ideal method of enforcing compliance with the law is to adopt an “enforcement pyramid”.⁵²⁰ Through this approach, regulators match the seriousness of the contravention with the severity of the sanction and resort to coercive sanctions only when the less interventionist methods would fail to ensure compliance. These measures should include both sanctions following contraventions as well as *ex-ante* tools which would allow the DPA to enforce the law.

An indicative list of the tools that should be made available to the DPA in the enforcement pyramid is below⁵²¹:

(i) Issuance of a Direction

The DPA should be given the power to issue directions from time to time as it may consider necessary to data fiduciaries and data processors either generally or to particular data fiduciaries and processors for discharging its functions under the law. Such fiduciaries and processors shall be bound to comply with these directions.⁵²²

(ii) Power to call for Information

The DPA will have the power to require a data fiduciary or data processor to provide such information, as may be necessary for performing its functions under the law. When calling for information, the DPA ought to specify the format and time in which such information is to be provided.⁵²³

⁵²⁰ See Chapter 50: Enforcing the Privacy Act, Australian Privacy Law and Practice (ALRC Report 108). The ALRC Report refers to J Braithwaite, To Punish or Persuade: Enforcement of Coal Mine Safety (1985); B Fisse and J Braithwaite, Corporations, Crime and Accountability (1993); C Dellit and B Fisse, Civil and Criminal Liability Under Australian Securities Regulation, The Possibility of Strategic Enforcement in G Walker and B Fisse (eds), Securities Regulation in Australia and New Zealand (1994) at p. 570; Comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee; Beni Chugh *et al*, Dvara Research Working Paper Series No. WP-2018-01 (July 2018) available at <<https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf>> (last accessed on 24 July 2018) at p. 9.

⁵²¹ Indicative tools set out below are adopted from the comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee; EU GDPR and commonly available enforcement tools seen under Indian statutes like SEBI Act, Insurance Act and so on. See also Beni Chugh *et al*, Dvara Research Working Paper Series No. WP-2018-01 (July 2018) available at <<https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf>> (last accessed on 24 July 2018) at pp 10-12.

⁵²² Adopted from the comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee; Beni Chugh *et al*, Dvara Research Working Paper Series No. WP-2018-01 (July 2018) available at <<https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf>> (last accessed on 24 July 2018) at p.11

⁵²³ Adopted from the comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee; Beni Chugh *et al*, Dvara Research Working Paper Series No. WP-2018-01 (July 2018) available at <<https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf>> (last accessed on 24 July 2018) at p.10.

(iii) Publication of Guidance

The DPA should inculcate a culture of openness where it encourages queries being posed to it by various stakeholders to clarify positions in the law. It could also issue guidance where it is of the view that a particular provision under the data protection law requires additional clarification. These responses could then be published on the DPA website to serve as guidance for the general public.⁵²⁴

(iv) Issuance of a Public Statement

The DPA may also issue public statements through its website regarding either trends of contraventions of the law by certain groups of data fiduciaries or of specific instances of contraventions to both heighten public awareness on the issue as well as to serve as a deterrent against infringements of the law.⁵²⁵

(v) Codes of Practice

The development of a good code of practice is fundamental to the functioning of a balanced data protection framework. A code of practice supplements the law, filling gaps with details that cannot be provided in legislation, thereby helping in better implementation of the principles the law is founded upon. The DPA will have the authority to issue codes of practices on its own, or it may approve codes of practice submitted by industry or trade associations representing the interests of data principals, sectoral regulators or statutory authorities. Before issuing or approving a code of practice, the DPA will be under an obligation to undertake a consultation process with appropriate sectoral regulators and other stakeholders, including data fiduciaries to take into account the developments taking place in the relevant industry. This is to ensure that codes of practice are issued in a transparent and democratic manner. Such codes of practice as issued by the DPA shall always be subject to the provisions of the applicable law.

The non-compliance with such codes of practice may be considered by the DPA, or any court or tribunal, in determining whether a data fiduciary or data processor (as the case may be and to the extent applicable) has violated provisions of the law. The concerned data fiduciary or data processor may however prove that it has adopted an equivalent or higher standard than the one stipulated in the relevant code of practice.

⁵²⁴ Adopted from the comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee; Beni Chugh *et al*, Dvara Research Working Paper Series No. WP-2018-01 (July 2018) available at <<https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf>> (last accessed on 24 July 2018) at p.10.

⁵²⁵ Adopted from the comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee; Beni Chugh *et al*, Dvara Research Working Paper Series No. WP-2018-01 (July 2018) available at <<https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf>> (last accessed on 24 July 2018) at p.11

(vi) Conducting Inquiries

The DPA may conduct an inquiry where it has a reasonable ground to believe that certain activities of the data fiduciary are likely to detrimentally affect the interests of a data principal; or that a data fiduciary has violated any of the provisions of the data protection law. To achieve this aim, the DPA should have the power to appoint inquiry officers to inquire into the affairs of the data fiduciary. The inquiry officer shall call for the requisite documents, books, records, etc. of the data fiduciary and examine any officer or employee of the data fiduciary for the purposes of inquiry. Moreover, the DPA should also have the power to conduct searches and seize documents and other material as may be required for the purposes of enforcement.

(vii) Injunctive Relief

Pursuant to its power of conducting an inquiry, the DPA shall have the powers to issue warnings, reprimands, order data fiduciaries to cease and desist from causing violations of the law, modify or temporarily suspend businesses or activities of data fiduciaries who are found to be in contravention of the law, suspend or discontinue any cross-border flow of personal data, cancel or suspend any registration granted by the DPA and take any other action as it may see fit to ensure compliance with the law.

(viii) Inter-sectoral coordination

It is relevant to mention that since the DPA will be dealing with a subject matter on which other regulators or authorities set up under a law made by the Parliament or any state legislature may also exercise concurrent jurisdiction, the DPA shall consult such regulators and authorities before taking any action under the proposed data protection legal framework and also enter into a memorandum of understanding with such regulators and authorities governing the coordination of such action.⁵²⁶

(c) Adjudication Wing of the DPA

In addition, the DPA shall also have a separate and independent Adjudication Wing which shall consist of such number of Adjudicating Officers as the Central Government may prescribe. The Central Government must undertake a capacity assessment exercise before determining the number of Adjudicating Officers who would be part of this office. Such officers should be individuals of integrity and ability and must have special knowledge of, and professional experience of not less than 7 years in areas related to constitutional law,

⁵²⁶ Adopted from the comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee; Beni Chugh *et al*, Dvara Research Working Paper Series No. WP-2018-01 (July 2018) available at <<https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf>> (last accessed on 24 July 2018) at pp 12, 14.

information technology law and policy, cyber and internet laws and related subjects.⁵²⁷ Further, the terms and conditions of appointment of such Adjudicating Officers must ensure their independence. The Adjudication Wing should function at arm's length from the remaining wings of the DPA which deal with legislative matters and executive enforcement. The Adjudicating Officers shall have the power to conduct an enquiry and adjudicate any dispute arising between data fiduciaries and data principals, including availing any compensation. Further, the Adjudicating Officer may also impose monetary penalties where the data fiduciary has contravened the provisions of the law.⁵²⁸

(d) Appellate Tribunal

An appellate tribunal shall be set up to hear and dispose of any appeals from the orders of the DPA and the orders of the Adjudicating Officers under the Adjudication Wing of the DPA. Such a tribunal should consist of a chairperson and such number of members as notified by the Central Government. The Central Government may also confer powers on an existing tribunal for this purpose if it believes that any existing tribunal is competent to discharge the functions of the appellate tribunal envisaged under the data protection law. The orders of the appellate tribunal will be finally appealable to the Supreme Court of India.

B. The Regulated Entities: Classification and Obligations

I. White Paper and Public Comments

The provisional view of the White Paper suggested the creation of differentiated obligations for certain entities whose processing activities create higher degrees of risk or may cause significant harm for better enforcement.⁵²⁹

Most commenters were in favour of some form of categorisation of entities to be regulated under the law. It was commonly suggested that fiduciaries processing sensitive personal data should be dealt with separately. Other criteria for categorisation included public or private nature of the entity, breadth of aggregation of data, inherent risks in the nature of the processing activity, scale of operations, turnover, sector of operations, range of products, and services offered. If a special category of data fiduciaries were to be created, a majority of the

⁵²⁷ Section 8, Competition Act; Section 15I, SEBI Act.

⁵²⁸ Inputs taken from the SEBI Act; Comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee; Beni Chugh *et al*, Dvara Research Working Paper Series No. WP-2018-01 (July 2018) available at <<https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf>> (last accessed on 24 July 2018) at p.16.

⁵²⁹ White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at Part IV, Chapter 2C.

In this context, the Committee also notes the Comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee as well as Beni Chugh *et al*, Dvara Research Working Paper Series No. WP-2018-01 (July 2018) available at <<https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf>> (last accessed on 24 July 2018).

commenters agreed that they should have additional obligations, such as mandatory registration, DPIAs, data audits, and a DPO. A few commenters suggested alternative obligations on entities such as maintaining records of processing activities, frequent supervision, higher reporting obligations, review or audit of data security and data breach mitigation plans.

The perspective on registration of data fiduciaries was split. Those who favoured it thought that it would assist in monitoring and identification of entities. Those who opposed it argued that it would add substantial compliance cost and an entry barrier, which would in turn discourage ease of doing business in India. Regarding audits, commenters were conflicted on whether they should be conducted internally or by empanelled external firms. Those who favoured some form of external audits argued that it ensured transparency, credibility, removal of bias, and accuracy. Most commenters favoured the requirement for a DPO in regulated entities. Some attempted to temper the requirement by arguing that the DPO need not be located in India. The functions that commenters sought to allocate to the DPO include advising, compliance monitoring, ensuring accountability, performing audits and DPIAs, cooperating with the regulator, training staff, grievance redressal, acting as the contact person on data protection matters, and monitoring security safeguards.

II. Analysis

(a) Significant Data Fiduciaries

The Committee is of the opinion that it is important to distinguish and place additional obligations on entities which are capable of causing significantly greater harm to data principals as a consequence of their data processing activities. This categorisation of data fiduciaries will enable the DPA to treat data fiduciaries who have the potential to cause greater harm on a separate track.

The categorisation will be based on an overall assessment of the following parameters: volume of the personal data being processed, nature of data (sensitive or not), volume of personal data processed, type of processing activity undertaken (collection, use, disclosure), turnover of the data fiduciary, the risk of harm resulting from any processing undertaken, whether the data fiduciary is making use of any new kind of technology to carry out the processing activity, or the presence of any other harm which is likely to cause harm to the data fiduciary. These broad parameters will be set out in the law and the DPA will have the power to lay down specific details/thresholds to identify such entities, who will be classified as significant data fiduciaries.

Significant data fiduciaries ought to have, at a minimum, the following additional obligations - (i) Registration with the DPA; (ii) DPIA; (iii) Record-keeping; (iv) Data audits; and (v) Appointment of DPO. However, where the DPA is of the view that processing undertaken by a data fiduciary (not being a significant data fiduciary) carries a risk of significant harm to data principals, it may notify the application of these obligations on such data fiduciaries.

(i) Registration

The DPA will have to oversee a large regulatory space criss-crossing different organisations in a variety of sectors. Consequently, it will be onerous for the DPA to identify each such data fiduciary that may cause significant harm. In order to solve this problem, significant data fiduciaries will have to register with the DPA. The process of registration is intended to be a notification by an entity which fulfils the threshold criteria of a significant data fiduciary, it is not akin to a licensing requirement to carry on business.

(ii) Data Protection Impact Assessment

The use of new technologies, large-scale profiling, and use of sensitive personal data like biometric and genetic information are activities with potential to endanger data principals' interests in the event of a security breach.⁵³⁰ Before commencing any of the aforementioned activities, significant data fiduciaries would be required to conduct an assessment of the impact such a project is likely to have on the data principals affected by such change and set out the means of reducing or eliminating such impact through a DPIA. The DPA would publish a list of situations when such an assessment would need to be conducted. Though the impact assessment is envisaged as an internal organisational measure, there may also be situations where an external data auditor (as discussed below) should be engaged by the fiduciary to carry out a DPIA. The DPA must determine what these situations are.

The DPIA should contain the following:

1. description of the nature, scope, context and purpose of processing;
2. necessity and proportionality of processing;
3. risks posed to the data principals' personal data and harms likely to be caused to a data principal; and
4. measures that could be deployed to reduce or eliminate these risks.

The DPIA must be submitted to the DPA who may then choose to advise the significant data fiduciary on the areas which may need further analysis or action on the part of the data fiduciary. It may direct the fiduciary to cease the processing or carry it out subject to conditions it imposes.

(iii) Record-keeping

Under the principle of accountability, data fiduciaries are required to be able to demonstrate that any processing undertaken by them are in accordance with data protection law. As a part of this obligation, it would often be necessary that verifiable and authentic records are

⁵³⁰ UK Information Commissioner's Office's Guide to the GDPR, Data protection impact assessments available at <<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>>, (last accessed on 26 April 2018).

maintained by them regarding the processing operations that they undertake. Nonetheless, for abundant caution, the Committee finds it appropriate that a separate obligation be in place requiring significant data fiduciaries to maintain accurate and up-to-date records regarding particularly important processing operations as well as the results of any security safeguard review, reports from data protection impact assessments and other aspects that may be specified by the DPA. This obligation would ensure that these fiduciaries are able to cooperate with the DPA and would permit monitoring of the relevant operations.⁵³¹ Given the volume, pervasiveness and risks of leakage of data related to processing by State entities, the Committee also finds it appropriate to mandatorily require such entities to maintain records.

(iv) Data Audits

Data audits should be undertaken by independent external auditors empanelled by the DPA to assess whether a significant data fiduciary's processing activities and policies are in compliance with the applicable data protection law. As highlighted by commenters, having external auditors will ensure transparency and credibility.⁵³² Besides, it will not be feasible for the DPA itself to conduct audits for all significant data fiduciaries. It is our view that a new profession of data auditors will have to be created to comply with norms in this law and other sector-specific regulation pertaining to data handling. The qualification of auditors should be determined by delegated legislation.⁵³³ Though this obligation is envisaged as recurring on a regular basis (for instance, annually) it is appropriate to empower the DPA to require data fiduciaries to conduct audits on other occasions in situations where it is likely that harm would be caused to data principals. In such situations, it is necessary for the DPA to appoint an auditor for this purpose.

A data audit shall include an analysis of compliance with obligations set out under the data protection law such as purpose and collection limitation, storage limitation, organisational and security measures undertaken, responses to grievance and requests, DPIAs undertaken, clarity of privacy policies and consent forms, and processing activities of children. On the basis of the audit, a rating in the form of a data trust score (indicating compliance with the obligations under the data protection law) may be assigned to such significant data fiduciaries by the data auditor having regard to any criteria that may be specified by the DPA in this regard.

⁵³¹ Recital 82, EU GDPR.

⁵³² UK Information Commissioner's Office, *Auditing Data Protection - A Guide to ICO Data Protection Audits* available at <<https://ico.org.uk/media/for-organisations/documents/2787/guide-to-data-protection-audits.pdf>> (last accessed on 30 April 2018); Adopted from comments in response to the White Paper submitted by Pramod Rao Citibank on 31 January 2018, available on file with the Committee.

⁵³³ By way of comparison, in the UK, the qualifications for an auditor are that they should be IIA (Institute of Internal Auditors) qualified and hold the ISEB (Information Systems Examination Board) Certificate in Data Protection (or be working towards those qualifications). Further, a range of skills and backgrounds including data protection casework, the banking sector, IT services and financial audit; UK Information Commissioner's Office, *Auditing Data Protection - A Guide to ICO Data Protection Audits* available at <<https://ico.org.uk/media/for-organisations/documents/2787/guide-to-data-protection-audits.pdf>> (last accessed on 30 April 2018). In Australia, under Section 26A(3), Privacy Act, 1988, the Privacy Commissioner for audit purposes, "may engage as consultants persons with suitable qualifications and experience. The terms and conditions on which a consultant is engaged are as determined by the Commissioner."

(v) Data Protection Officer

Given that significant data fiduciaries may process considerably sensitive and large amounts of personal data, it is essential that they appoint a person who facilitates compliance with data protection laws by monitoring and advising these fiduciaries as well as acts as a point of contact with the DPA. The eligibility and qualification requirements of the DPO will be specified by way of delegated legislation. The functions allocated to such DPO could include compliance monitoring, developing and ensuring robust compliance and accountability procedures, cooperating with the DPA, training staff, conducting DPIAs, grievance redressal, monitoring security safeguards, and maintaining records, etc.

C. Penalties, Compensation and Offences

I. White Paper and Public Comments

The White Paper considered several models of imposition of a monetary penalty on data fiduciaries found to be in violation of the data protection law, which included a per-day penalty, a penalty based on the discretion of the adjudicatory body which would be subject to a fixed upper limit and finally one where the discretion is subject to an upper limit which is a variable parameter. The White Paper provisionally concluded that the highest form of deterrence in relation to civil penalties may be where a per day civil penalty is imposed subject to a fixed upper limit or a percentage of the total worldwide turnover of the defaulting data controller of the previous financial year, whichever is higher. Further, the White Paper concluded that an individual may be given a right to seek compensation when she has suffered a loss or damage as a result of an infringement of the data protection law.⁵³⁴

Some commenters suggested that penalties should either have a fixed upper limit, or be based on a percentage of the turnover of the entity. According to the commenters, some contraventions by fiduciaries which ought to warrant penalties include: unlawful processing of personal data, unauthorised disclosure of personal data, failure to implement security measures, and violation of individual rights.

Commenters were also of the view that data principals who suffer “material or non-material damage” may be considered where “non-material damage or harm” should include breach of privacy, mental distress, reputational harm, discrimination, etc.

Further, in the case of an offence, commenters suggested that fines along with imprisonment should be imposed on data fiduciaries in certain, specific instances of violations of the data protection law where *mala fide* intent or recklessness is involved. A few commenters also suggested that only wilful non-compliance with the orders of the DPA should be punished with criminal liability.

⁵³⁴ White Paper of the Committee of Experts on a Data Protection Framework for India, available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at Part IV, Chapter 4.

II. Analysis

(a) Burden of Proof and Accountability

When seeking a remedy under the law, it would have to be demonstrated that the data fiduciary has violated any provisions of the law or any harm has been suffered by the data principal as a result of such violation. Once this has been established, to mitigate any liability, the data fiduciary would have to prove, *inter alia*, that it has complied with the provisions of the law and undertaken all necessary and requisite measures to prevent any harm. It is necessary to note, however, that in relation with the conditions for the validity of consent, the burden of proof should specifically be placed on the data fiduciary.

(b) Penalties

The Adjudicating Officer under the Adjudication Wing of the DPA should have the power of imposing monetary penalties on infringing data fiduciaries. Civil penalties have been acknowledged as an effective method of ensuring deterrence.⁵³⁵ Penalty imposed should be such which will make it unprofitable for data fiduciaries to be engaging in the wrongful act in the future and will be proportional to the harm suffered by the data principal. Obviously, the amount cannot be set at either extreme of excessive penalisation which would decrease business activity in the sector or minimal penalisation which would not have deterrent value. The Committee is of the view that a penalty of up to a certain percentage of the total worldwide turnover in the preceding financial year of the data fiduciary or a fixed amount set by the law, whichever is higher (and as applicable depending on the type of data fiduciary involved) should be imposed for major infractions of law. The Committee is cognisant of the fact that in today's day and age, data fiduciaries, especially companies incorporated in India, forming part of a group may be processing personal data for their parent, subsidiary or other companies within the same group. In such cases, the Committee is of the view that such group companies may also be penalised where they may have benefitted from any unlawful processing undertaken by the said data fiduciaries. Consequently, the proposed legal framework will set out the formulation to reflect this understanding.⁵³⁶ Furthermore, the law will also set out penalties based on different formulations for violations involving failure to comply with any request pursuant to data principal rights, failure to furnish reports, information, etc. as mandated under the law.

The final determination of the amount within the range provided should be dependent on factors which would include the following:

⁵³⁵ Max Minzner, Why Agencies Punish, 53(3) William and Mary Law Review (2012); Michelle Welsh, Civil Penalties and Responsive Regulation: The Gap Between Theory And Practice, 33(3) Melbourne University Law Review (2009).

⁵³⁶ A similar approach is seen in the EU GDPR. Moreover, even in the Indian context, Section 27(b), Competition Act imposes a penalty of “not more than ten percent of the average of the turnover for the last three preceding financial years” for abuse of dominant position. Further, Section 43A, Competition Act penalises up to one percent of the total turnover or the assets, of a combination which has not furnished information to the CCI.

- (i) the nature, gravity and duration of the infringement which would depend on the nature, scope or purpose of the processing and the number and sensitivity of data principals affected;
- (ii) whether the infringement was intentional or grossly negligent;
- (iii) efforts made by the data fiduciary to mitigate the damage caused to the data principals;
- (iv) the technical and organisational measures implemented by the data fiduciary including adherence to the code of practice; and
- (v) any relevant previous infringement by the data fiduciary.

(c) Compensation

There needs to be certainty in the ascription of liability so that the data principals are not made to run from pillar to post in search of finding the relevant fiduciary or processor in the link who was responsible for the damage caused. Therefore, joint and several liability to pay compensation would be attached to the data fiduciary and its processors with penalty being imposed so long as an infringement has been proven. Therefore, at the first instance, the aggrieved data principal will receive the compensation amount due to her. Thereafter, the division of liabilities of paying compensation will become a second order question.

A remedy needs to be provided under the law to compensate data principals for the harm caused to them due to infringements under the data protection law. The factors for deciding on the quantum of compensation being awarded could be largely similar to the factors set out under the penalties section. These may include the following:

- (i) Nature, duration and extent of non-compliance or violation of legal obligation by data fiduciary;
- (ii) Nature and extent of harm suffered by the data principal due to the default;
- (iii) The intentional or negligent character of the violation;
- (iv) Whether the data fiduciary is sufficiently transparent in its data processing activities;
- (v) Whether the data fiduciary, or the data processor as the case may be took any measures to mitigate the damage suffered by the data principal;
- (vi) Amount of gain or unfair advantage to the data fiduciary, whether quantifiable, due to the default;
- (vii) Repetitive nature of the default- whether first time or a subsequent breach and whether there has been any previous instance of such breach;
- (viii) Failure to operate policies, procedures and practices to protect personal data;
- (ix) Nature of the personal data involved.

(d) Offences

Offences created under the data protection law should be linked to any intentional or reckless behaviour, or to damage caused with knowledge to the data principals in question. Some acts which may be treated as an offence would be: (i) obtaining, transfer, disclosure and sale of personal and sensitive personal data in violation of the provisions of the data protection law such that it caused harm to the data principal; (ii) re-identification and processing of previously de-identified personal data. Such offences may be made cognizable and non-bailable and may be tried by the relevant jurisdictional court. In cases of offences committed by companies, the person in-charge of the conduct of the business of the company, and in the cases of offences by a government department, the head of the department should be held responsible. However, liability should not be imposed on such persons if they can prove that such offence was committed without her consent or that they put in all reasonable efforts to prevent such commission of an offence.

RECOMMENDATIONS

- The data protection law will set up a DPA which will be an independent regulatory body responsible for the enforcement and effective implementation of the law. Broadly, the DPA shall perform the following primary functions: (i) monitoring and enforcement; (ii) legal affairs, policy and standard setting; (iii) research and awareness; (iv) inquiry, grievance handling and adjudication. **[Chapter X of the Bill]**
- The DPA is vested with the power to categorise certain fiduciaries as significant data fiduciaries based on their ability to cause greater harm to data principals as a consequence of their data processing activities. This categorisation will be based on an assessment of volume of the personal data being processed, nature of personal data, type of processing activity undertaken, turnover of the data fiduciary, the risk of harm, and the type of technology used to undertake processing. **[Section 38 of the Bill]**
- Significant data fiduciaries will have to undertake obligations such as: (i) Registration with the DPA; (ii) Data Protection Impact Assessments; (iii) Record-keeping; (iii) Data audits; and (iv) Appointment of DPO. The DPA can require that any other data fiduciaries may have to undertake these obligations as well. **[Sections 33, 34, 35, 36 and 38 of the Bill]**
- The following enforcement tools shall be made available to the DPA: (i) Issuance of directions; (ii) Power to call for information; (iii) Publication of guidance; (iv) Issuance of public statement; (v) Codes of Practice; (vi) Conducting inquiry; (vii) Injunctive Relief; (viii) Inter-sectoral coordination. **[Chapter X of the Bill]**
- Pursuant to its powers of inquiry, the DPA has wide-ranging powers including issuing warnings, reprimands, ordering data fiduciaries to cease and desist, modify or temporarily suspend businesses or activities of data fiduciaries who are found to be in contravention of the law etc. **[Section 64 of the Bill]**
- The DPA's Adjudication Wing shall be responsible for adjudication of complaints between data principals and data fiduciaries. **[Section 68 of the Bill]**
- The Central Government shall establish an appellate tribunal or grant powers to an existing appellate tribunal to hear and dispose of any appeal against an order of the DPA. Appeals against orders of the appellate tribunal will be to the Supreme Court of India. **[Sections 84 and 87 of the Bill]**
- Penalties may be imposed on data fiduciaries and compensation may be awarded to data principals for violations of the data protection law. The penalties imposed would be an amount up to the fixed upper limit or a percentage of the total worldwide turnover of the preceding financial year, whichever is higher. Offences created under the law should be limited to any intentional or reckless behaviour, or to damage caused with knowledge to the data principals in question. **[Sections 69, 70, 71, 72, 73, 75 and Chapter XIII of the Bill]**

SUMMARY OF RECOMMENDATIONS

Jurisdiction and Applicability

- The law will have jurisdiction over the processing of personal data if such data has been used, shared, disclosed, collected or otherwise processed in India. However, in respect of processing by fiduciaries that are not present in India, the law shall apply to those carrying on business in India or other activities such as profiling which could cause privacy harms to data principals in India. Additionally, personal data collected, used, shared, disclosed or otherwise processed by companies incorporated under Indian law will be covered, irrespective of where it is actually processed in India. However, the data protection law may empower the Central Government to exempt such companies which only process the personal data of foreign nationals not present in India. **[Sections 2 and 104 of the Bill]**
- The law will not have retrospective application and it will come into force in a structured and phased manner. Processing that is ongoing after the coming into force of the law would be covered. Timelines should be set out for notifications of different parts of the law to facilitate compliance. **[Section 97 of the Bill]**

Processing

- The definition of personal data will be based on identifiability. The DPA may issue guidance explaining the standards in the definition as applied to different categories of personal data in various contexts. **[Section 3(29) of the Bill]**
- The law will cover processing of personal data by both public and private entities. **[Sections 3(13) and 3(15) of the Bill]**
- Standards for anonymisation and de-identification (including pseudonymisation) may be laid down by the DPA. However, de-identified data will continue to be within the purview of this law. Anonymised data that meets the standards laid down by the DPA would be exempt from the law. **[Sections 3(3), 3(16) and 61(6)(m) of the Bill]**
- Sensitive personal data will include passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric and genetic data, and data that reveals transgender status, intersex status, caste, tribe, religious or political beliefs or affiliations of an individual. However, the DPA will be given the residuary power to notify further categories in accordance with the criteria set by law. **[Sections 3(35) and 22 of the Bill]**
- Consent will be a lawful basis for processing of personal data. However, the law will adopt a modified consent framework which will apply a product liability regime to consent thereby making the data fiduciary liable for harms caused to the data principal. **[Section 12 of the Bill]**
- For consent to be valid it should be free, informed, specific, clear and capable of being withdrawn. For sensitive personal data, consent will have to be explicit. **[Sections 12 and 18 of the Bill]**
- A data principal below the age of eighteen years will be considered a child. Data fiduciaries have a general obligation to ensure that processing is undertaken keeping the best interests of the child in mind. Further, data fiduciaries capable of causing significant harm to children will be identified as guardian data fiduciaries. All data fiduciaries (including guardian data fiduciaries) shall adopt appropriate age verification mechanism and obtain parental consent. Furthermore, guardian data fiduciaries, specifically, shall be barred from certain practices. Guardian data fiduciaries exclusively offering counselling services or other similar services will not be required to take parental consent. **[Section 23 of the Bill]**
- The principle of granting protection to community data has been recognised by the Committee. This should be facilitated through a suitable law which is recommended to be enacted by the Government of India in the future.

Obligations of Data Fiduciaries

- The relationship between the “data subject” and the “data controller” is to be reformulated as a fiduciary relationship between the “data principal” and the “data fiduciary”. **[Sections 3(13) and 3(14) of the Bill]**
- All processing of personal data by data fiduciaries must be fair and reasonable. **[Section 4 of the Bill]**
- The principles of collection and purpose limitation will apply on all data fiduciaries unless specifically exempted. **[Sections 5 and 6 of the Bill]**
- Processing of personal data using big data analytics where the purpose of the processing is not known at the time of its collection and cannot be reasonably communicated to the data principal can be undertaken only with explicit consent.
- A principle of transparency is incumbent on data fiduciaries from the time the data is collected to various points in the interim. Most prominently, a data fiduciary is obliged to provide notice to the data principal no later than at the time of the collection of her personal data. **[Sections 8 and 28 of the Bill]**
- There shall be obligations of data quality and storage limitation on data fiduciaries. However, the responsibility to ensure that the personal data provided is accurate will rest on the data principal. **[Sections 9 and 10 of the Bill]**
- There will be a provision of personal data breach notification to the DPA and in certain circumstances, to the data principal. **[Section 32 of the Bill]**
- Data security obligations will be applicable. **[Section 31 of the Bill]**

Data Principal Rights

- The right to confirmation, access and correction should be included in the data protection law. **[Sections 24 and 25 of the Bill]**
- The right to data portability, subject to limited exceptions, should be included in the law. **[Section 26 of the Bill]**
- The right to object to processing; right to object to direct marketing, right to object to decisions based on solely automated processing, and the right to restrict processing need not be provided in the law for the reasons set out in the report.
- The right to be forgotten may be adopted, with the Adjudication Wing of the DPA determining its applicability on the basis of the five-point criteria as follows:
 - (i) the sensitivity of the personal data sought to be restricted;
 - (ii) the scale of disclosure or degree of accessibility sought to be restricted;
 - (iii) the role of the data principal in public life (whether the data principal is publicly recognisable or whether they serve in public office);
 - (iv) the relevance of the personal data to the public (whether the passage of time or change in circumstances has modified such relevance for the public); and
 - (v) the nature of the disclosure and the activities of the data fiduciary (whether the fiduciary is a credible source or whether the disclosure is a matter of public record; further, the right should focus on restricting accessibility and not content creation). **[Section 27 of the Bill]**
- The right to be forgotten shall not be available when the Adjudication Wing of the DPA determines upon conducting the balancing test that the interest of the data principal in limiting the disclosure of her personal data does not override the right to freedom of speech and expression as well as the right to information of any other citizen. **[Section 27 of the Bill]**
- Time-period for implementing such rights by a data fiduciary, as applicable, shall be specified by the DPA. **[Section 28 of the Bill]**

Transfer of Personal Data outside India

- Cross border data transfers of personal data, other than critical personal data, will be through model contract clauses containing key obligations with the transferor being liable for harms caused to the principal due to any violations committed by the transferee. **[Section 41(1)(a) of the Bill]**
- Intra-group schemes will be applicable for cross-border transfers within group entities. **[Section 41(1)(a) of the Bill]**
- The Central Government may have the option to green-light transfers to certain jurisdictions in consultation with the DPA. **[Section 41(1)(b) of the Bill]**
- Personal data determined to be critical will be subject to the requirement to process only in India (there will be a prohibition against cross border transfer for such data). The Central Government should determine categories of sensitive personal data which are critical to the nation having regard to strategic interests and enforcement requirements. **[Section 40(2) of the Bill]**
- Personal data relating to health will however be permitted to be transferred for reasons of prompt action or emergency. Other such personal data may additionally be transferred on the basis of Central Government approval. **[Section 41(3) of the Bill]**
- Other types of personal data (non-critical) will be subject to the requirement to store at least one serving copy in India. **[Section 40(1) of the Bill]**

Allied Laws

- Various allied laws are relevant in the context of data protection because they either require or authorise the processing of personal data for different objectives.
- All relevant laws will have to be applied along with the data protection law, as the latter will be the minimum threshold of safeguards for all data processing in the country. In the event of any inconsistency between data protection law and extant legislation, the former will have overriding effect.
- The proposed data protection framework replaces Section 43A of the IT Act and the SPD Rules issued under that provision. Consequently, these must be repealed together with consequent minor amendments. **[First Schedule of the Bill]**
- The RTI Act prescribes a standard for privacy protection in laying out an exemption to transparency requirements under Section 8(1)(j). This needs to be amended to clarify when it will be activated and to harmonise the standard of privacy employed with the general data protection statute. **[Second Schedule of the Bill]**
- The Committee has identified a list of 50 statutes and regulations which have a potential overlap with the data protection framework. Concerned ministries may take note of this and ensure appropriate consultation to make complementary amendments where necessary.
- The Aadhaar Act needs to be amended to bolster data protection. Suggested amendments for due consideration are contained in the Appendix to this Report.

Non-Consensual Grounds of Processing

- Functions of the State: Welfare functions of the state will be recognised as a separate ground for processing. Processing activities carried out by the State under law will be covered under this ground, ensuring that it is in furtherance of public interest and governance. However, only bodies covered under Article 12 of the Constitution may rely on this ground. Processing towards activities that may not be considered part of a welfare functions would, however, not be permitted. Thus, the availability of this ground is restricted to certain entities and certain functions to avoid vagueness in the law. **[Sections 13 and 19 of the Bill]**
- Compliance with Law or Order of Court or Tribunal: Compliance with law or order of court or tribunal will be recognised as a separate ground for processing to avoid inconsistency with obligations under other laws, regulations and judicial orders. The word ‘law’ shall be construed to mean laws, ordinances, orders, bye-law, rules, regulations and notifications that have statutory authority. Order of court or tribunal would be restricted to Indian courts and tribunals. Obligations imposed by contract, foreign law and foreign judicial orders shall not be permitted to be processed under this ground. **[Sections 14 and 20 of the Bill]**
- Prompt Action: Prompt action will be recognised as a separate ground for processing. It should receive a strict interpretation and only be applied in critical situations where the individual is incapable of providing consent and the processing is necessary to meet emergency situations. **[Sections 15 and 21 of the Bill]**
- Employment: Employment will be recognised as a separate ground for processing. This ground should be invoked only where processing under consent would involve disproportionate effort or where the employment relation makes consent inappropriate, and will permit processing even where employment-related activities are not authorised under any of the other grounds of processing such as compliance with law. **[Sections 16 of the Bill]**
- Reasonable Purpose: Reasonable purpose is a residuary ground for processing activities which are not covered by other grounds like consent, compliance with law, prompt action and public function but are still useful to society. The ambit of the provision would be limited to those purposes which are whitelisted by the DPA to guide data fiduciaries. **[Section 17 of the Bill]**

Exemptions

- Security of the State: The data protection law will enable an exemption to the processing of personal or sensitive personal data if it is necessary in the interest of the security of the state. Any restriction must be proportionate and narrowly tailored to the stated purpose. The Central Government should expeditiously bring in a law for the oversight of intelligence gathering activities. **[Section 42 of the Bill]**
- Prevention, Detection, Investigation and Prosecution of Contraventions of Law: The data protection law should provide an exemption for prevention, detection, investigation and prosecution of contraventions of law (including protection of revenue). In order to invoke the exemption, the law enforcement agencies must be authorised by law. **[Section 43 of the Bill]**
- Disclosure for the Purpose of Legal Proceedings: The disclosure of personal data necessary for enforcing a legal right or claim, for seeking any relief, defending any charge, opposing any claim or for obtaining legal advice from an advocate in an impending legal proceeding would be exempt from the application of the data protection law. General obligations of security and fair and reasonable processing will continue to apply. **[Section 44 of the Bill]**
- Research Activities: The research exemption is not envisaged as a blanket exemption. Only those obligations that are necessary to achieve the object of the research will be exempted by the DPA. This assessment is contextual and dependent on the nature of the research. **[Section 45 of the Bill]**
- Personal or Domestic Purposes: A narrowly tailored exemption for purely personal or domestic processing of data should be incorporated in the data protection law. It would provide a blanket exemption from the application of the data protection law. **[Section 46 of the Bill]**
- Journalistic Activities: To strike a balance between freedom of expression and right to informational privacy, the data protection law would need to signal what the term ‘journalistic purposes’ signifies, and how ethical standards for such activities would need to be set. Where these conditions are met, an exemption should be provided. **[Section 47 of the Bill]**
- Manual Processing by Small Entities: Since the risk of privacy harms being caused are higher when personal data is processed through automated means, an exemption will be made in the data protection law for manual processing by data fiduciaries that are unlikely to cause significant harm and would suffer the heaviest relative burdens from certain obligations under this law. **[Section 48 of the Bill]**

Enforcement

- The data protection law will set up a DPA which will be an independent regulatory body responsible for the enforcement and effective implementation of the law. Broadly, the DPA shall perform the following primary functions: (i) monitoring and enforcement; (ii) legal affairs, policy and standard setting; (iii) research and awareness; (iv) inquiry, grievance handling and adjudication. **[Chapter X of the Bill]**
- The DPA is vested with the power to categorise certain fiduciaries as significant data fiduciaries based on their ability to cause greater harm to data principals as a consequence of their data processing activities. This categorisation will be based on an assessment of volume of the personal data being processed, nature of personal data, type of processing activity undertaken, turnover of the data fiduciary, the risk of harm, and the type of technology used to undertake processing. **[Section 38 of the Bill]**
- Significant data fiduciaries will have to undertake obligations such as: (i) Registration with the DPA; (ii) Data Protection Impact Assessments; (iii) Record-keeping; (iii) Data audits; and (iv) Appointment of DPO. The DPA can require that any other data fiduciaries may have to undertake these obligations as well. **[Sections 33, 34, 35, 36 and 38 of the Bill]**
- The following enforcement tools shall be made available to the DPA: (i) Issuance of directions; (ii) Power to call for information; (iii) Publication of guidance; (iv) Issuance of public statement; (v) Codes of Practice; (vi) Conducting inquiry; (vii) Injunctive Relief; (viii) Inter-sectoral coordination. **[Chapter X of the Bill]**
- Pursuant to its powers of inquiry, the DPA has wide-ranging powers including issuing warnings, reprimands, ordering data fiduciaries to cease and desist, modify or temporarily suspend businesses or activities of data fiduciaries who are found to be in contravention of the law etc. **[Section 64 of the Bill]**
- The DPA's Adjudication Wing shall be responsible for adjudication of complaints between data principals and data fiduciaries. **[Section 68 of the Bill]**
- The Central Government shall establish an appellate tribunal or grant powers to an existing appellate tribunal to hear and dispose of any appeal against an order of the DPA. Appeals against orders of the appellate tribunal will be to the Supreme Court of India. **[Sections 84 and 87 of the Bill]**
- Penalties may be imposed on data fiduciaries and compensation may be awarded to data principals for violations of the data protection law. The penalties imposed would be an amount up to the fixed upper limit or a percentage of the total worldwide turnover of the preceding financial year, whichever is higher. Offences created under the law should be limited to any intentional or reckless behaviour, or to damage caused with knowledge to the data principals in question. **[Sections 69, 70, 71, 72, 73, 75 and Chapter XIII of the Bill]**

No. 3(6)/2017-CLES
Government of India
Ministry of Electronics & Information Technology

Electronics Niketan
New Delhi-110003
Dated : 31st July, 2017

OFFICE MEMORANDUM

Subject: Constitution of a Committee of Experts to deliberate on a data protection framework for India

The Government of India is cognizant of the growing importance of data protection in India. The need to ensure growth of the digital economy while keeping personal data of citizens secure and protected is of utmost importance.

2. It has thus been decided to constitute a Committee of Experts under the Chairmanship of Justice B N Srikrishna, Former Judge, Supreme Court of India, to identify key data protection issues in India and recommend methods of addressing them. The constitution of the group and terms of reference are as follows:

- | | |
|---|-------------------|
| a) Justice B N Srikrishna, Former Judge,
Supreme Court of India | - Chairperson |
| b) Smt. Aruna Sundararajan, Secretary,
Department of Telecom | - Member |
| c) Dr Ajay Bhushan Pandey, CEO, UIDAI | - Member |
| d) Dr Ajay Kumar, Addl Secretary, MeitY | - Member |
| e) Prof Rajat Moona, Director, IIT, Raipur | - Member |
| f) Dr. Gulshan Rai,
National Cyber Security Coordinator | - Member |
| g) Prof. Rishikesh T. Krishnan,
Director, IIM, Indore | - Member |
| h) Dr. Arghya Sengupta, Research Director,
Vidhi Centre for Legal Policy | - Member |
| i) Ms. Rama Vedashree, CEO, DSCI | - Member |
| j) Joint Secretary, MeitY | - Member Convener |

3. **Terms of Reference**

- a) To study various issues relating to data protection in India
- b) To make specific suggestions for consideration of the Central Government on principles to be considered for data protection in India and suggest a draft data protection bill.

Contd...2/-

:2:

4. The Committee may co-opt other members in the Group for their specific inputs.

5. MeitY shall in consultation with the Chairperson and members, collect necessary information and provide it to the Committee within 8 weeks of the date of this OM to enable it to start its deliberations on the subject.

6. The Committee shall endeavour to submit its report as expeditiously as possible.

7. The expenditure towards TA/DA in connection with the meetings of the group in respect of the official members will be borne by their respective Ministries/Departments. Domestic travel in respect of non-official members would be permitted by Air India (Business Class) and the expenditure would be met by MeitY.

(Rakesh Maheshwari)
Group Coordinator,
Cyber Law & UIDAI

To

- 1) Justice B N Srikrishna, Former Judge Supreme Court of India
- 2) Smt. Aruna Sundararajan, Secretary,
- 3) Dr Ajay Bhushan Pandey, CEO, UIDAI
- 4) Dr Ajay Kumar, Addl Secretary, MeitY
- 5) Prof Rajat Moona, Director, IIT, Raipur
- 6) Dr. Gulshan Rai, National Cyber Security Coordinator
- 7) Prof. Rishikesha T. Krishnan, Director, IIM, Indore
- 8) Dr. Arghya Sengupta, Research Director, Vidhi Centre for Legal Policy
- 9) Ms. Rama Vedashree, CEO, DSCI
- 10) Joint Secretary, MeitY

Copy to:

- i) PS to Hon'ble, Minister (E&IT)
- ii) PS to Hon'ble MoS (E&IT)
- iii) OSD to Secretary, MeitY
- iv) All Group Coordinators, MeitY

How can Privacy Policy documents be designed for better communication?

These suggestions have been arrived at after studying Privacy Policy documents of over twenty platforms, including online marketplaces, search engines, social networks, etc. Their chief objective is to improve the presentation of these textual documents, making them easier to consume and understand.

These suggestions will each improve these documents along one or more of the following parameters:

APPROACHABILITY

Minimising the intimidating nature of such documents, to encourage engagement

COMPREHENSIBILITY

Simplifying and organising the content to make it more easily and widely understandable

HELPFULNESS

Making the text an active assistant in engagement and comprehension, and not just a passive vehicle for the content

LEGIBILITY & READABILITY

Optimising the typography and page layout for easy and effortless perusal

CONSCIENTIOUSNESS

Prioritising users' right to be informed about their data and its use, and giving them granular control over what they consent to.

One Simplifying Text

- Simplify phrasing, with crisp sentences and easier words.

- Rephrase section headings as questions.

EXAMPLES:

We use the information we collect to show you content that's relevant, interesting and specific to you. Here's how:

Who has access to my information?

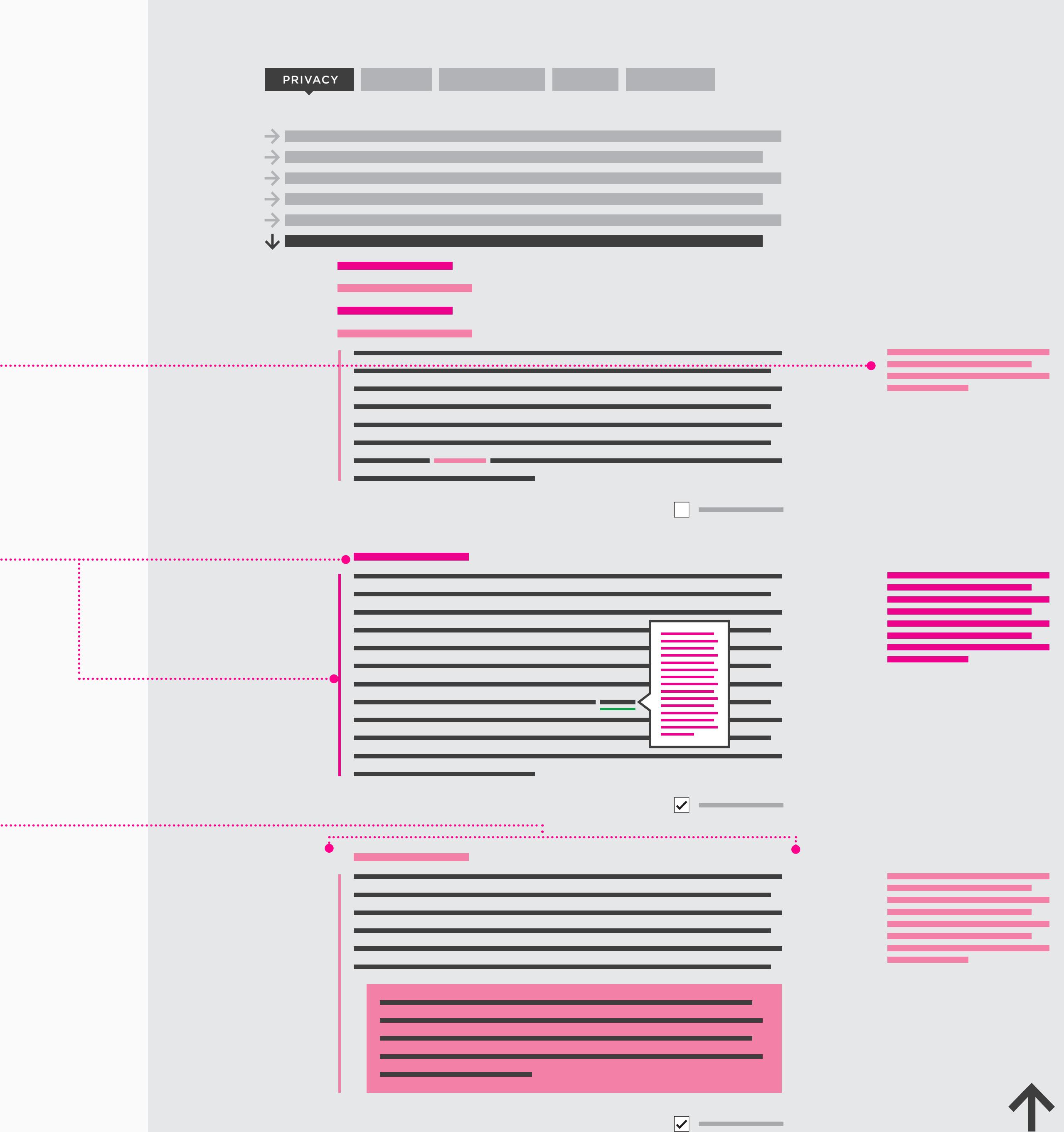
Two Structuring Content, with Intuitive Navigation

- Provide a separate page for all Privacy-related information, as a distinct tab.
 - Categorise the content into sections, as a collapsible list of links.
 - Segregate content within a section into sub-sections, wherever possible, as a collapsible list of links.
 - Provide intra- or inter- document links, when a reference to a different section within the Privacy Policy document, or in another document, is made.
 - Collapse tangential, instantial or incidental information into mouse-over or pop-up links.
 - User input fields (for permissions) should be opt-in, instead of opt-out, (for instance: no pre-checked boxes).
 - These requests for permissions should be de-bundled, with separate input fields appearing alongside the clause relevant to them.
 - Provide a link to return to the top of the page, at all points of scrolling.

Three

Designing for Ease (Macro)

- Supply a brief, plain-language summary beside each section, with the salient points of the section. This would be non-binding, and only intended as an aid.
- Use non-textual design elements, such as icons, colour codes etc.—strategically, to aid meaning.
- Fix column widths at 55-65 characters (including spaces), leaving generous amounts of white space on all sides of the text column(s), as far as possible.



Four Designing for Ease (Micro)



- Use a font which is easily legible.
- Provide adequate line spacing.
- Differentiate between different types of text (section headings, sub-section headings, body text etc.) such that they are immediately distinguishable from one another. This can be done through:
 - Font attributes: create clear differences in weight, size and colour
 - Positioning: increase distance from dissimilar content, decrease distance from similar content, create visual ‘clubs’
 - Lists: use ordered or unordered lists, wherever possible.
 - Use typographic treatment consistently—the same kind of content must have the same appearance throughout the document.

Five Creating Emphasis (for Disclaimers, Onerous Clauses etc.)



- Use proper capitalisation—avoid all-uppercase.
- Create, and consistently follow, a visual style for emphasis that is instantly noticeable, without compromising on readability. Outlined below are a few ways to achieve that:
 - Visual markers: Fields of colour, icons, etc.
 - Font attributes: differentiate from body text in weight, size and/or colour.
 - Positioning: break alignment from the rest of the text, to draw attention.

EXAMPLE:

What information do we collect?

When you sign up for or use <Example>, you give us certain information voluntarily. This includes your name, email address, phone number, profile photo, comments, and any other information you give us. You can also choose to share with us location data or photos.

If you link your Facebook or Google account or accounts from other third party services to Pinterest, we also get information from those accounts (such as your friends or contacts). The information we get from those services depends on your settings and their privacy policies, so please check what those are.

<Example> may contain links to other sites.
<Example> is not responsible for the privacy policies and/or practices on other sites. When linking to another site you should read the privacy policy stated on that site. This Privacy Policy only governs information collected by <Example>.

Six Providing language support

- Provide options to view the document in the common languages of the regions where the service is available.

Seven Optimising across Devices

- Design for common break-points, ensuring maximum reader-friendliness across all common devices.

Eight Providing for Offline Use

- Supply an offline version of the document—if the original privacy policy is provided online—with the same content organisation, hierarchy and typographic treatment.

Nine Presenting in Other forms

- While all the above suggestions are for textual documents, platforms are also encouraged to arrive at audio-visual ways in which Privacy Policies can be explained. This would greatly aid user engagement and comprehension.

ANNEXURE C

List of Allied Laws Impacted by a Draft Data Protection Law in India

A. Information Technology Laws

1. Indian Telegraph Act, 1885
2. Information Technology Act, 2000
3. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data Or Information) Rules, 2011

B. Land and Taxation Laws

1. The Right to Fair Compensation and Transparency in Land Acquisition Act, 2013
2. Income Tax Act, 1961
3. Central Goods and Services Tax Act, 2017
4. The Black Money (Undisclosed Foreign Income and Assets) And Imposition of Tax Act, 2015

C. Criminal Justice Laws

1. Prisons Act, 1894
2. Identification of Prisoners Act 1920
3. Official Secrets Act, 1923

D. Law relating to International Relations

1. United Nations (Privileges and Immunities) Act, 1947

E. Alternative Dispute Resolution

1. The Arbitration and Conciliation Act, 1996

F. Health Laws

1. The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002
2. Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994
3. The Mental Health Act, 1987
4. Persons with Disabilities (Equal Opportunities, Protection of Rights and Full Participation) Act, 1995

G. Intellectual Property Laws

1. Trademarks Act, 1999
2. Copyright Act, 1957

H. Symbols, Records and Statistics Laws

1. The Collection of Statistics Act, 2008
2. The Census Act, 1948

I. Trade and Commerce Laws

1. Bureau of Indian Standards Act, 1986

J. Defence Laws

1. The Enemy Property Act, 1968
2. The Defence of India Act, 1962

K. Labour and Employment Laws

1. The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013
2. Employees' Provident Fund and Miscellaneous Provisions Act, 1952
3. Employees' State Insurance Act, 1948

L. Corporate and Financial Laws

1. Reserve Bank of India Act, 1935
2. Insurance Act, 1938
3. Banking Regulation Act, 1934
4. National Bank for Agriculture and Rural Development Act, 1981
5. National Housing Bank, 1987
6. Small Industries and Development Bank of India Act, 1989
7. Payment and Settlement Systems Act, 2007
8. Depositories Act, 1996
9. Companies Act, 2013
10. Insolvency and Bankruptcy Code, 2016
11. Securities & Exchange Board of India Act, 1992
12. Competition Act, 2002
13. Securities Contracts (Regulation) Act
14. Credit Information Companies (Regulation) Act, 2005
15. Limited Liability Partnership Act, 2008
16. Prevention of Money Laundering Act, 2002

M. Miscellaneous

1. The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016
2. Consumer Protection Act, 1986
3. Right of Children to Free and Compulsory Education Act, 2009
4. Right to Information Act, 2005
5. The Telecom Regulatory Authority of India Act, 1997
6. Foreign Contribution (Regulation) Act, 2010
7. The Prohibition of Benami Property Transactions, 1988
8. Indian Evidence Act, 1872

APPENDIX

Suggested amendments to the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

The following amendments have been suggested to the Aadhaar Act from a data protection perspective. They must be read alongside Chapters XI and XII of the proposed data protection bill which deal with enforcement action and individual remedies. The rationale for these amendments have been explained in the Report from pages 98 to 101. The amendments may be duly considered by the Government and suitable legislation introduced as deemed appropriate.

1. Amendment of section 2. — In section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (hereinafter referred to as the principal Act),

(1) in place of the current clause (a), the following clause shall be substituted, namely:—

“(a) “Aadhaar number” means a twelve-digit identification number issued to an individual under sub-section (3) of section 3 and includes any alias thereof generated in a manner specified by regulations”

(2) after clause (b), the following clauses shall be inserted, namely:—

“(ba) “Adjudicating Officer” means an adjudicating officer appointed under sub-clause (1) of section 33B;”

“(bb) “Appellate Tribunal” means the Telecom Disputes Settlement and Appellate Tribunal established under section 14 of the Telecom Regulatory Authority of India Act, 1997;”

(3) after clause (m), the following clause shall be inserted, namely:—

“(ma) “Entities in the Aadhaar ecosystem” includes enrolling agencies, Registrars, requesting entities, offline verification-seeking entities and any other entity or group of entities as specified by the Authority;”

(4) after clause (p), the following clauses shall be inserted, namely:—

“(pa) “Offline verification” means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by regulations;”

“(pb) “Offline verification-seeking entity” means any entity desirous of undertaking offline verification of an Aadhaar number holder.”

2. Amendment of section 4.— In place of the current sub-section (3) of section 4 of the principal Act, the following sub-section (3) of section 4 shall be substituted, namely:—

“(3) An Aadhaar number, in physical or electronic form subject to authentication or offline verification and other conditions, as may be specified by regulations, may be accepted as proof of the identity of the Aadhaar number holder for any purpose.”

3. Amendment of section 8.— (1) In place of sub-section (1) of section 8 of the principal Act, the following sub-sections shall be substituted, namely:—

“8. Authentication of Aadhaar number .—

(1) The Authority shall perform authentication of the Aadhaar number of an Aadhaar number holder on the request of a requesting entity only when such authentication is:

- (a) mandated pursuant to law made by Parliament;
- (b) required by a public authority for performing a public function, subject to prior approval of the Authority on such conditions as the Authority may deem fit.

(1A) In determining whether to grant approval under sub-section (1), the Authority shall take into account the following factors:

- (a) the nature of the interest of the requesting entity seeking authentication;
- (b) the standards of security employed by the requesting entity; and
- (c) any other factor which is relevant in protecting the privacy of an Aadhaar number holder.

(1B) The Authority may, by regulations, classify requesting entities into such categories as may be necessary to determine whether such requesting entity may request an Aadhaar number holder for the Aadhaar number itself during authentication or only any alias or aliases thereof.”

(2) After clause (b) of sub-section (2) of section 8 of the principal Act, the following clause shall be inserted, namely: —

“(c) ensure the availability of alternate and viable means of identification of an Aadhaar number holder in case of a failure to authenticate on account of

illness, injury or infirmity owing to old age or otherwise, and any technical reasons as may be specified.”

4. Insertion of section 8A.— After section 8 of the principal Act, the following section 8A shall be inserted, namely:—

“(8A) Offline verification of Aadhaar number.—

- (1) Any offline verification of an Aadhaar number holder shall take place on the basis of consent provided to such verification by the Aadhaar number holder.
- (2) Any offline verification-seeking entity shall,
 - (a) obtain the consent of an individual before verifying him offline, in such manner as may be specified by regulations; and
 - (b) ensure that the demographic information or any other information collected from the individual for offline verification, if any, is only used for the purpose of such verification.
- (3) An offline verification-seeking entity shall inform the individual undergoing offline verification the following details with respect to offline verification, in such manner as may be specified by the regulations, namely:—
 - (a) the nature of information that may be shared upon offline verification;
 - (b) the uses to which the information received during offline verification may be put by the offline verification requesting entity;
 - (c) alternatives to submission of information requested for, if any.
- (4) An offline verification-seeking entity shall not:
 - (a) subject an Aadhaar number holder to authentication;
 - (b) collect, use or store an Aadhaar number or biometric information of any individual for any purpose;
 - (c) take any action contrary to any obligations on it, specified by regulations.

5. Substitution of section 21.— In place of the current section 21 of the principal Act, the following section 21 shall be substituted, namely:—

“21. Officers and other employees of Authority.—

- (1) The Authority shall determine the number, nature and categories of other officers and employees required for the discharge of its functions under this Act.
- (2) The salaries and allowances payable to, and the other terms and conditions of service of, the officers and other employees of the Authority shall be such, as may be specified.”

6. Amendment of section 23.— After section 23 of the principal Act, the following sections shall be inserted, namely:—

“23A. Power of Authority to issue directions.—

- (1) The Authority may, in exercise of its powers or for discharge of its functions under this Act, or any rules or regulations made hereunder, issue such directions from time to time to entities in the Aadhaar ecosystem, as it may consider necessary.
- (2) Any direction issued under sub-section (1) for providing alternate and viable means of identification in case of failure to authenticate shall have effect, notwithstanding anything contained in any law in force.
- (3) If the Authority finds, on the basis of material in its possession, that any person has violated, or is likely to violate, any provisions of this Act, or any rules or regulations made thereunder, it may pass an order requiring such person to cease and desist from committing or causing such violation, or give such directions as may be necessary for the purpose of securing compliance with that condition or provision.”

“23B. Power of Authority to conduct inquiry.—

- (1) The Authority may conduct an inquiry where it has reasonable grounds to believe that—
 - (a) the activities of an entity in the Aadhaar ecosystem are being conducted in a manner which is detrimental to, or in violation of the privacy of an individual or an Aadhaar number holder; or
 - (b) any entity in the Aadhaar ecosystem has violated any of the provisions of this Act or the rules prescribed or the regulations specified or directions issued by the Authority thereunder.
- (2) For the purpose of sub-section (1), the Authority shall, by an order in writing, appoint an Inquiry Officer to conduct the inquiry where such order shall set out inter alia the scope of inquiry and reasons for commencing inquiry and the Inquiry Officer shall prepare an inquiry report to be submitted to the Authority.
- (3) Every person acting under the direct authority of the entity in the Aadhaar ecosystem, service provider or a contractor where services are being obtained by or provided to the entity in the Aadhaar ecosystem, as the case may be, shall be bound to produce before the Inquiry Officer,

all such documents, records and data in their custody or power and to furnish to the Inquiry Officer any statement and information relating to the affairs of the entity in the Aadhaar ecosystem as the Inquiry Officer may require within the time stipulated by such officer.

- (4) The Inquiry Officer shall undertake the inquiry only after providing a written notice to the persons referred to in sub-section (3) stating the reasons for the inquiry and the relationship between the entity in the Aadhaar ecosystem and the scope of the investigation.
- (5) The Inquiry Officer may keep in its custody any documents, records and data referred to in sub-section (3) for six months and thereafter shall return the same to the persons concerned.
- (6) Without prejudice to the provisions of this Act or any other law, an Inquiry Officer may examine on oath, any person acting under the direct authority of the entity in the Aadhaar ecosystem, or a service provider, or a contractor where services are being obtained by or provided to the entity in the Aadhaar ecosystem, as the case may be, for conducting an inquiry.

“23C. Powers of Search and Seizure.—

- (1) Where the Authority has reasonable grounds to believe that—
 - (a) any person referred to in sub-section (3) of section 23B has failed or omitted to produce any documents, records or data in her custody or power; or
 - (b) any such documents, records or data mentioned in clause (a) of sub-section (1) are likely to be tampered with, altered, mutilated, manufactured, falsified or destroyed; or
 - (c) a contravention of any provision of this Act has been committed or is likely to be committed by an entity of the Aadhaar ecosystem,

it may authorise any officer of the Authority not below the rank equivalent to that of a Gazetted Officer of the Central Government (hereinafter referred to as “Authorised Officer”) to—

- (i) enter and search any building or place where she has reason to suspect that such documents, records or data are kept;
- (ii) break open the lock of any box, locker, safe, almirah or other receptacle for exercising the powers conferred by clause (i) where the keys thereof are not available;
- (iii) access any computer, computer resource, or any other device containing or suspected to be containing data;
- (iv) seize all or any such documents, records or data found as a result of such search;
- (v) place marks of identification on such documents, records or databases or make extracts or copies of the same.

- (2) The Authorised Officer may requisition the services of any police officer or of any officer of the Central Government, or of both, as the case may be, for assistance related to any of the purposes specified in sub-section (1) and it shall be the duty of every such officer to comply with such requisition.
- (3) The Authorised Officer may, where it is not practicable to seize any such document, record or data specified in sub-section (1), serve an order on the person who is in immediate possession or control thereof that such person shall not remove, part with or otherwise deal with it except with the previous permission of such officer.
- (4) The Authorised Officer may, during the course of the search or seizure, examine on oath any person who is found to be in possession or control of any documents, records or data, and any statement made by such person during such examination may thereafter be used in evidence in any proceeding under this Act.
- (5) The documents, records or data seized under sub-section (1) shall not be retained by the Authorised Officer for a period exceeding six months from the date of the seizure unless the approval of the Authority for such retention is obtained.
- (6) The Authority shall not authorise the retention of documents, records or data for a period exceeding thirty days after all the proceedings under this Act, for which the said documents, records or data are relevant, are completed.
- (7) The person from whose custody the documents, records or data are seized under sub-section (1) may make copies thereof, or take extracts therefrom, in the presence of the Authorised Officer at such place and time as may be designated.
- (8) If a person legally entitled to the documents, records or data seized under sub-section (1) objects for any reason to the approval given by the Authority under sub-section (5), such person may make an application to the Appellate Tribunal stating her objection and requesting for the return of the same.
- (9) On receipt of the application under sub-section (8), the Appellate Tribunal may, after giving the parties an opportunity of being heard, pass such order as it thinks fit.
- (10) The provisions of the Code of Criminal Procedure, 1973 (2 of 1974) relating to searches and seizures shall apply, so far as may be, to every search and seizure made under sub-section (1).
- (11) Without prejudice to the generality of the foregoing, rules may be prescribed in relation to the process for search and seizure under this section as may be deemed fit by the Authority.

“23D. Action to be taken by Authority pursuant to an inquiry.—

- (1) On receipt of a report under sub-section (2) of section 23B, the Authority may, after giving such opportunity to the entity in the Aadhaar ecosystem

to make a representation in connection with the report as the Authority deems reasonable, by an order in writing—

- (a) issue a warning to the entity in the Aadhaar ecosystem where the business or activity is likely to violate the provisions of this Act;
 - (b) issue a reprimand to the entity in the Aadhaar ecosystem where the business or activity has violated the provisions of this Act;
 - (c) require the entity in the Aadhaar ecosystem to cease and desist from committing or causing any violation of the provisions of this Act;
 - (d) require the entity in the Aadhaar ecosystem to modify its business or activity to bring it in compliance with the provisions of this Act;
 - (e) temporarily suspend or discontinue business or activity of the entity in the Aadhaar ecosystem which is in contravention of the provisions of this Act;
 - (f) initiate proceedings under section 33A of this Act;
 - (g) make a complaint under section 47 of this Act;
 - (h) require the entity in the Aadhaar ecosystem to take any such action in respect of any matter arising out of the report as the Authority may think fit.
 - (i) issue any other direction as it deems fit under sub-section (3) of section 23A of this Act;
- (2) An entity in the Aadhaar ecosystem aggrieved by an order made under this section by the Authority, except an order under clause (f) and (g) of sub-section (1), may prefer an appeal to the Appellate Tribunal.”
7. In place of the current section 25 of the principal Act, the following section shall be substituted, namely:—
- “25. Other fees and revenues.—**
- The fees or revenue collected by the Authority shall be credited to a fund called the Unique Identification Authority of India Fund to be managed by the Authority.”
8. In place of the current sub-section (4) of section 29 of the principal Act, the following sub-section (4) shall be substituted, namely:—
- “29. Restriction on sharing information.—**

- (4) No Aadhaar number, demographic information or photograph collected or created under this Act in respect of an Aadhaar number holder shall be published, displayed or posted publicly, except for purposes, if any, as may be specified.

Provided, nothing in this sub-section shall apply to core biometric information which shall only be governed by sub-section (1)."

9. Insertion of Chapters after Chapter VI.—After Chapter VI of the principal Act, the following Chapters shall be inserted, namely:—

**"CHAPTER VIA
CIVIL PENALTIES**

33A. Penalty for failure to comply with provisions of this Act, rules, regulations and directions.—

Whoever fails to comply with any provision of this Act, the rules or the regulations made hereunder or directions issued by the Authority under the provisions of this Act, or fails to furnish any information, document, or return of report required by the Authority, shall be liable to a civil penalty which may extend to one crore rupees for each contravention and in case of a continuing failure, with additional penalty which may extend to ten lakh rupees for every day during which the failure continues after the first contravention.

33B. Power to adjudicate.—

- (1) For the purposes of adjudication under section 33A and imposing a penalty thereunder, the Authority shall appoint any officer, not below the rank of a Joint Secretary to the Government of India, to be an Adjudicating Officer for adjudicating disputes in the manner prescribed by the Central Government.
- (2) The proceedings under sub-section (1) can only be initiated by the Authority against entities in the Aadhaar ecosystem.
- (3) While conducting the proceedings the Adjudicating Officer shall,—
 - (a) provide the entities in the Aadhaar ecosystem against whom a penalty is proposed to be levied, an oral hearing;
 - (b) have the power to summon and enforce the attendance of any person acquainted with the facts and circumstances of the case to give evidence or to produce any document which, in the opinion of the Adjudicating Officer, may be useful for or relevant to the subject matter of the proceedings.
- (4) Based on the information received pursuant to sub-section (3), if the Adjudicating Officer is satisfied that any entity in the Aadhaar ecosystem has failed to comply with any provision of this Act, the rules or the regulations made hereunder or directions issued by the Authority under the provisions of this Act, or has failed to furnish any information, document, or return of report required by the Authority, the Adjudicating Officer may, by order, impose such

penalty as he thinks fit in accordance with the provisions of section 33A.

- (5) Every Adjudicating Officer shall have the powers of a civil court, for the purposes of—
- Sections 193 and 228 of the Indian Penal Code, 1860;
 - Sections 345 and 346 of the Code of Criminal Procedure, 1973;
 - Order XXI of the Code of Civil Procedure, 1908.

CHAPTER VIB APPEALS

33C. Appeals to Appellate Tribunal.—

- Any person aggrieved by an order passed by an Adjudicating Officer under sub-section (4) of section 33B, may prefer an appeal before the Appellate Tribunal.
- Every appeal under sub-section (1) shall be filed within a period of forty-five days from the date of receipt of the order appealed against and it shall be in such form and manner and shall be accompanied by such fee as may be prescribed.
- On receipt of an appeal under sub-section (1), the Appellate Tribunal may, after giving the parties to the appeal an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.
- The Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the Adjudicating Officer.
- Any appeal filed under sub-section (1) shall be dealt with by the Appellate Tribunal as expeditiously as possible and every endeavour shall be made by it to dispose of the appeal within six months from the date on which it is presented to it.
- The Appellate Tribunal may, for the purpose of examining the legality or propriety or correctness of any order or decision of the Adjudicating Officer, either on its own motion or otherwise, call for the records relevant to disposing of such appeal and make such orders as it thinks fit.

33D. Procedure and powers of the Appellate Tribunal.—

The provisions of sections 14I to 14K (both inclusive), 16 and 17 of the Telecom Regulatory Authority of India Act, 1997 (24 of 1997) shall *mutatis mutandis* apply to the Appellate Tribunal in the discharge of its functions under this Act, as they apply to it in the discharge of its functions under the Telecom Regulatory Authority of India Act, 1997 (24 of 1997).

33E. Orders passed by Appellate Tribunal to be executable as a decree.—

- (1) An order passed by the Appellate Tribunal under this Act shall be executable by the Appellate Tribunal as a decree of a civil court, and for this purpose, the Appellate Tribunal shall have all the powers of a civil court.
- (2) Notwithstanding anything contained in sub-section (1), the Appellate Tribunal may transmit any order made by it to a civil court having local jurisdiction and such civil court shall execute the order as if it were a decree made by that court.

33F. Penalty for willful failure to comply with orders of Appellate Tribunal.—

If any person willfully fails to comply with the order of the Appellate Tribunal, he shall be punishable with a fine which may extend to one lakh rupees, and in case of a second or subsequent offence with a fine which may extend to two lakh rupees, and in the case of continuing contravention with an additional fine which may extend to two lakh rupees for every day during which such default continues.

33G. Appeal to Supreme Court.—

- (1) Notwithstanding anything contained in the Code of Civil Procedure, 1908 (5 of 1908) or in any other law, an appeal shall lie against any order, not being an interlocutory order, of the Appellate Tribunal to the Supreme Court only if it raises a substantial question of law.
- (2) No appeal shall lie against any decision or order made by the Appellate Tribunal which the parties have consented to.
- (3) Every appeal under this section shall be preferred within a period of forty-five days from the date of the decision or order appealed against.

33H. Recovery of penalty or compensation.—

- (1) For the purpose of this Act, the Authority shall, by an order in writing, appoint at least one officer or employee as a Recovery Officer who shall be empowered to seek the assistance of the local district administration while exercising the powers under this section.
- (2) Where any person fails to comply with— an order of the Adjudicating Officer imposing a penalty under the provisions of this Act, the Recovery Officer may recover from such person the aforesaid amount in any of the following ways, in descending order of priority, namely—
 - (a) attachment and sale of the person's movable property;

- (b) attachment of the person's bank accounts;
 - (c) attachment and sale of the person's immovable property;
 - (d) arrest and detention of the person in prison;
 - (e) appointing a receiver for the management of the person's movable and immovable properties.
- (3) For the purpose of such recovery, the provisions of section 220 to section 227, and sections 228A, 229 and 232, the Second and Third Schedules of the Income Tax Act, 1961 (43 of 1961) and the Income Tax (Certificate Proceedings) Rules, 1962, as in force from time to time, in so far as may be, shall apply with necessary modifications as if the said provisions and rules—
- (a) were the provisions of this Act; and
 - (b) referred to the amount due under this Act instead of to income tax under the Income Tax Act, 1961 (43 of 1961).
- (4) In this section, the movable or immovable property or monies held in a bank account shall include property or monies which meet all the following conditions—
- (a) property or monies transferred by the person without adequate consideration;
 - (b) such transfer is made:
 - (i) on or after the date on which the amount in the certificate drawn up under section 222 of the Income Tax Act, 1961 (43 of 1961) had become due; and
 - (ii) to the person's spouse, minor child, son's wife or son's minor child.
 - (c) such property or monies are held by, or stand in the name of, any of the persons referred to in sub-clause (b), including where they are so held or stand in the name of such persons after they have attained the age of majority.

33I. Civil Court not to have jurisdiction.—

No civil court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an Adjudicating Officer appointed under this Act or the Appellate Tribunal is empowered, by or under this Act to determine, and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.”

10. Amendment of sections 38 and 39.— In sections 38 and 39 of the principal Act, for the words “imprisonment for a term which may extend to three years”, the

words “imprisonment for a term which may extend to ten years” shall be substituted.

11. Substitution of section 40.— In place of the current section 40 of the principal Act, the following section 40 shall be substituted, namely:—

“40. Penalty for unauthorised use by requesting entity.—

Whoever, being a requesting entity, fails to obtain the consent of an individual before collecting his identity information for the purposes of authentication in contravention of clause (a) of sub-section (2) of Section 8, shall be punishable with imprisonment which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees, or with both.”

12. Insertion of sections 41A, 41B, 41C, 41D.— After section 41 of the principal Act, the following sections shall be inserted, namely:—

“41A. Penalty for failure to obtain consent for authentication or offline verification.—

Whoever, being a requesting entity or an offline verification seeking entity, fails to obtain the consent of an individual before collecting his identity information for the purpose of authentication in contravention of clause (a) of sub-section (2) of Section 8, or necessary information for the purpose of offline verification in contravention of clause (a) of sub-section (2) of section 8A, shall be punishable with imprisonment which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees, or with both.

41B. Penalty for unauthorised use of core biometric information.—

Whoever uses core biometric information collected or created under this Act for any purpose other than generation of Aadhaar numbers and authentication under this Act, shall be punishable with imprisonment which shall not be less than three years but which may extend to ten years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to fifty lakh rupees, or with both.

41C. Penalty for unauthorised publication of Aadhaar number or photograph.—

Whoever wrongfully publishes, displays or posts publicly, Aadhaar numbers collected or created under this Act, or demographic information or photograph in respect of an Aadhaar number holder, except for the

purposes specified under this Act or regulations, shall be punishable with imprisonment which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees, or with both.”

41D. Penalty for offline verification-seeking entities.—

Whoever, being an offline verification-seeking entity, collects, stores or uses the Aadhaar number of an Aadhaar number holder or makes an Aadhaar number holder undergo authentication, unless mandated pursuant to any law enacted by Parliament, shall be punishable with imprisonment which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees, or with both.”

13. Amendment of section 42.— In section 42 of the principal Act, for the words “imprisonment for a term which may extend to one year”, the words “imprisonment for a term which may extend to three years” shall be substituted.

14. Amendment of section 53.— In section 53, in sub-section (2), —

(1) after clause (d), the following clauses shall be added, namely:—

“(da) the process for search and seizure under sub-section (11) of section 23C;”

(2) In section 53, in sub-section (2), after clause (g), the following clauses shall be added, namely:—

“(ga) the manner of appointment of an adjudicating officer under sub-section (1) of section 33B;”

“(gb) the form, manner, and fee for an appeal to be filed under sub-section (2) of section 33C.”

15. Amendment of section 54.— In section 54 of the principal Act, in sub-section (2),

(1) after clause (a), the following clauses shall be added, namely :—

“(aa) the manner of generating an alias of Aadhaar under clause (a) of section 2;”

“(ab) the entities or group of entities in the Aadhaar ecosystem under clause (ma) of section 2;”

“(ac) the modes of offline verification of Aadhaar number under clause (pa) of section 2;”

(2) after clause (f), the following clauses shall be added, namely :—

“(fa) the classification of requesting entities under sub-section (1B) of section 8;”

“(fb) the technical reasons necessitating the specification of alternate and viable means of identification under clause (c) of sub-section (2) of Section 8;”

“(fc) the manner of obtaining consent under clause (a) of sub-section (2) of section 8A;”

“(fd) the manner of providing information to the individual undergoing offline verification under clause sub-section (3) of section 8A;”

“(fd) the obligations of offline verification-seeking entities under clause (c) of sub-section (4) of section 8A;”

(3) after clause (u), the following clauses shall be added, namely :—

“(ua) the purposes for which Aadhaar number, demographic information or photograph collected may be published, displayed or posted publicly under sub-section (4) of Section 29;”

16. Amendment of section 57.— In the proviso to section 57 of the principal Act, after the words “under section 8” the following words and numbers shall be inserted namely :—

“, section 8A”

Vikash

From: Rama Vedashree (DSCI) [rama@dsci.in]
Sent: Friday, July 27, 2018 2:37 PM
To: js.gopal@meity.gov.in; Srikrishna BN
Cc: Ajay Sawhney; Vikash Chourasia
Subject: My Note on the final Version of Draft Bill received on 26th July 2018
Attachments: Dissent Note Rama Vedashree.docx; Copy of Sensitive Personal Data Final.xlsx

Dear Sirs

I wish to thank you both for giving me the opportunity to participate in the Committee Deliberations, and giving me a patient hearing in all the meetings and submissions, during the last one year.

It has been a tremendous learning for me to participate in the meetings and learn from all the committee members and the chair.

Iam fully supportive of Govt bringing a strong Data Protection and Privacy regime. Data Security Council of India (A NASSCOM Initiative) owes its genesis to driving best practices in Data Protection comparable with global models in the Industry. We have pioneered a Privacy Framework, and Credentials and Certification Program namely DSCI Privacy Framework and DCPP, DCPLA, which is widely adopted by Industry members across IT, Banking and Telecom sectors in India. We also have been deeply contributing to India's readiness in Cyber Security and Privacy, and conformance to Global Data Protection Regimes by our Industry Members. Privacy by Design is a concept which is very key to the Privacy charter of DSCI team and wish to assure you we will scale our efforts in Privacy Capability Building in the country on the same.

Iam grateful to the Chair and committee for incorporating several of my inputs into the Final Draft Bill.

Wish to place on record my special appreciation of Vidhi Legal Research team who worked tirelessly in Drafting the white paper and consultation exercise and helping draft the final versions.

My two colleagues Vinayak Godse, and Anand Krishnan contributed a lot to my research and contributions in the committee too.

While Iam very supportive of the overall Bill, I disagree with three provisions. Iam enclosing a note on the same. Would appreciate if it is placed as record in the Committee's Submission to Government.

However I wish to reassure you, that while I will continue to pursue advocating with Government as they undertake consultations in its enactment and enforcement, I stay committed to contributing deeply to help Government and our Industry members in getting ready to the new Data Protection Legislation and ensuring Privacy of Indians is protected. I also respect the chair and committee's endeavours in building a consensus, and the constraints in accepting all my inputs.

Thank You and assuring you of my support in implementation of the final Personal Data Protection Law.

Best Regards
Rama Vedashree

Note on THE PERSONAL DATA PROTECTION BILL, 2018

Rama Vedashree

Data Security Council of India (DSCI) and its Industry members have been advocating for a data privacy and protection law in the country for the last several years. We believe, the digital economy should primarily aim to benefit citizens, and the technology sector is fully supportive as the growth and proliferation of Information and Digital technologies is linked to citizen's feeling safe, secure and assured in the digital environment. DSCI since its inception has been working towards promoting data protection and is committed to equipping the industry through its capacity building initiatives to raise the threshold of privacy practices in India.

To ensure growth of the digital economy while keeping personal data of citizens secure and protected, it is important that as a country we take a balanced view that can meet the twin imperatives of safety and security of Indian data as well as enable the flow of global data into and from India.

The committee of experts under the chairmanship of Justice B.N. Srikrishna, has been working tirelessly for a year to achieve the goals laid down before us. The extensive Public Consultation and soliciting feedback from all stakeholders in India and across the world, and comprehensive review of inputs received has been a highlight of the Committee's deliberations. The framework proposed by the committee incorporates numerous provisions that lay emphasis on demonstration of accountability and re-establishing trust between entities and end consumers in the digital ecosystem.

But, with respect to certain provisions inscribed in the bill, I have a fundamental disagreement. This disagreement exists with respect to three provisions in particular.

First, the draft bill in its present form places restrictions on cross border flow of personal data. Under section 40(1) of the bill, this restriction translates into storing a copy of all personal data within India, while section 40 (2) completely restricts the cross-border flow of personal data for sensitive data categorised as critical personal data by the central government at its discretion, without inscribing guiding principles for this determination in the bill.

This approach is not only regressive but against the fundamental tenets of our liberal economy. Moreover, the inclusion of such restrictions in a bill that should focus primarily on empowering Indians with rights and remedies to uphold their right to privacy, seems out of place.

The committee report in chapter 6, projects localisation as tool for domestic market development. This narrative seems fuelled by unfounded apprehensions and assumptions, rather than evidence and reasoning.

We as a country and Industry have been advocating the imperative of free flow of data and talent across borders. This is the foundation of the \$167 billion IT-BPM industry represents and is India's largest foreign exchange earner (\$110B in 2017-18). IT-BPM Service providers in India process financial, healthcare and other data of citizens and companies in the US, EU, and elsewhere in the world and have created employment for over 4 million people. Mandating localization may potentially become a trade barrier and the key markets for the industry

could mandate similar barriers on data flow to India, which could disrupt the IT-BPM industry. We are not only a Global hub for corporations from more than 80 countries, but also the destination for leading Global Corporations for R&D, Product Development and Analytics, Shared Services. We are also one of the largest growing technology start-up hub in the world, who from India are offering their innovative solutions and services to global geographies often leveraging global cloud platforms, thanks to the fundamental principle of Cross Border Data Flows and Internet economy.

Second, I disagree with the categorisation of financial data and password as sensitive personal data under section 3(35) of the bill. The guiding principles as mentioned in the report under chapter 3, for determining sensitivity are broad and can possibly be used to justify the inclusion of any type of data to this category of personal data. The concept of Sensitive Personal Data is primarily used for providing higher level protection to the data subject from instances of profiling, discrimination and infliction of harm that are identity driven. Neither financial data nor passwords fall into this category. It is also important to note, out of the 68 countries that presently have an overarching data protection regulation none have categorised financial data or passwords as sensitive personal data. These include countries from Asia Pacific, Europe and the Middle East.¹

Third, the inclusion of criminal offences under chapter XIII of the draft bill is draconian. The Draft Bill and the Report, with steep fines and compensations advocate penalties which are sufficient to achieve the imperative of having deterrent penalties. The inclusion of criminal offences along with the fines and compensation is excessive and would impact the enforcement mechanism greatly. The enforcement tools should enable swift assessment and action to keep the process lean and approachable for the common man.

In addition to the above-mentioned points, the report under chapter 7 and the associated appendix, suggests sweeping amendments to the Aadhaar Act; these need a thorough review. I suggest a separate public consultation exercise by the government to examine these amendments.

I also request Government to publish the Bill, and the Report on MeitY's website, and conduct a round of Industry and stakeholder consultations before enacting the same.

¹Please refer annexure 1.

Sensitive Personal Data Around the World
As per July 2018

**Source: Data Protection Laws
of The World, DLA Piper**

<https://www.dlapiperdataprotection.com/index.htm>

No.	Country	Financial Data	Passwords	Health Data	Genetic Data	Racial & Ethnic Origin	Religious Belief	Political Belief	Sex Life	Biometric Data
1	Angola	No	No	Yes	Yes	Yes	No	Yes	Yes	No
2	Argentina	No	No	Yes	No	Yes	Yes	Yes	Yes	No
3	Australia	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No
4	Austria	No	No	No	No	Yes	Yes	Yes	Yes	No
5	Belgium	No	No	Yes	No	Yes	Yes	Yes	Yes	No
6	Bosnia and Herzegovina	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
7	Bulgaria	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No
8	Cape Verde	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes
9	China	No	No	No	No	Yes	Yes	Yes	No	Yes
10	Costa Rica	No	No	No	No	Yes	Yes	Yes	Yes	No
11	Croatia	No	No	Yes	No	Yes	Yes	Yes	Yes	No
12	Cyprus	No	No	Yes	No	Yes	Yes	Yes	Yes	No
13	Czech Republic	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
14	Denmark	No	No	Yes	No	Yes	Yes	Yes	Yes	No
15	Estonia	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
16	Finland	No	No	Yes	No	Yes	Yes	Yes	Yes	No
17	France	No	No	Yes	No	Yes	Yes	Yes	Yes	No
18	Germany	No	No	Yes	No	Yes	Yes	Yes	Yes	No
19	Ghana	No	No	Yes	No	Yes	Yes	Yes	Yes	No
20	Gibraltar	No	No	Yes	No	Yes	Yes	No	Yes	No
21	Greece	No	No	Yes	No	Yes	Yes	Yes	Yes	No
22	Guernsey	No	No	Yes	No	Yes	Yes	Yes	Yes	No
23	Honduras	No	No	Yes	No	Yes	Yes	Yes	No	No

24	Hungary	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	No
25	Iceland	No	No	Yes	No						
26	Ireland	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	No
27	Israel	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	No
28	Italy	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	No
29	Japan	No	No	Yes	No	Yes	No	No	No	No	No
30	Jersey	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	No
31	Latvia	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	No
32	Lesotho	No	No	Yes							
33	Lithuania	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No
34	Luxembourg	No	No	Yes	No						
35	Macau	No	No	Yes	No						
36	Macedonia	No	No	Yes							
37	Madagascar	No	No	Yes							
38	Malaysia	No	No	Yes	No	No	Yes	Yes	Yes	No	No
39	Malta	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	No
40	Mauritius	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	No
41	Mexico	No	No	Yes	No						
42	Monaco*	No	No	Yes	No						
43	Montenegro	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	No
44	Morocco	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No
45	Netherlands	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	No
46	Nigeria	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	No
47	Norway	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	No
48	Philippines	No	No	Yes	No						
49	Poland	No	No	Yes	No						
50	Portugal	No	No	Yes	No						
51	Qatar	No	No	Yes	No	Yes	Yes	No	No	No	No
52	Romania	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	No
53	Russia	No	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes
54	Seychelles	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	No

56	Slovak Republic	No	No	No	No	Yes	Yes	Yes	No	Yes
57	South Africa	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes
58	South Korea	No	No	Yes	Yes	No	Yes*	Yes	No	No
59	Spain	No	No	Yes	No	Yes	Yes	Yes	Yes	No
60	Sweden	No	No	Yes	No	Yes	Yes	Yes	Yes	No
61	Switzerland	No	No	Yes	No	Yes	Yes	Yes	Yes	No
62	Taiwan	No	No	Yes	Yes	No	No	No	Yes	No
63	Trinidad and Tobago	No	No	Yes	No	Yes	Yes	Yes	Yes	No
64	Turkey	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes
65	UAE - Dubai (DIFC)	No	No	Yes	No	Yes	Yes	Yes	Yes	No
66	Ukraine	No	No	Yes	No	Yes	Yes	Yes	Yes	No
67	United Kingdom	No	No	Yes	No	Yes	Yes	Yes	Yes	No
68	Uruguay	No	No	Yes	No	Yes	Yes	Yes	Yes	No

Monoco: Sensitive personal data is not expressly defined under the DPL but it is deemed to be:

South Korea

The law uses the narrower term "creed" instead of Religious Beliefs

Vikash

From: Prof. Rishikesha T Krishnan [rishi@iimdr.ac.in]
Sent: Friday, July 27, 2018 3:19 PM
To: vikash
Subject: Fwd: Reservations regarding the Report of the Data Protection Committee

----- Forwarded message -----

From: Prof. Rishikesha T Krishnan <rishi@iimdr.ac.in>
Date: Fri, Jul 27, 2018, 3:11 PM
Subject: Reservations regarding the Report of the Data Protection Committee
To: B.N. Srikrishna <bnsrikrishna@gmail.com>
Cc: js gopal <js.gopal@meity.gov.in>

Dear Justice Srikrishna,

It has been a privilege for me to be a member of this Committee that has undertaken the most challenging task of envisioning a robust data protection framework for India. I thank you for providing an environment where free discussion of all issues was possible. I particularly laud your efforts to undertake extensive consultation with all stakeholders.

I am in broad agreement with the conclusions in the report and the accompanying draft bill.

However, I have reservations regarding the following which I would like to place on record. I would be grateful if these reservations could be recorded appropriately so that these are available to anyone who reads the report.

1. The requirement that every data fiduciary should store one live, serving copy of personal data in India is against the basic philosophy of the Internet and imposes additional costs on data fiduciaries without a proportional benefit in advancing the cause of data protection [Chapter 6 of the report].
2. The observations and recommendations regarding the Aadhaar Act are outside the scope of the committee's work.[Chapter 7 of the report].

Regards,

Rishikesha T. Krishnan

THE DATA PROTECTION BILL, 2018¹

A Bill to establish rights of individuals vis-a-vis their personal data and to codify the law governing personal data including collection, use, storage, sharing, processing and disclosure of personal data by all entities:

to create an ecosystem to enhance the flow of data for the sustained growth of the digital economy;

to advance human rights, promote economic mobility and economic growth by giving individuals more control over their personal data and protecting the informational privacy of individuals and preventing potential harms and misuse of any individuals' personal data, and

to align Indian data protection laws with international standards, allowing India to retain and strengthen its competitiveness in the international market.

BE it enacted by Parliament in the Sixty-Eighth Year of the Republic of India as follows:

CHAPTER I

Preliminary

- 1. (1)** This Act may be called the Data Protection Act, 2018.

¹ This is a working document to holistically represent the different aspects of our vision at Dvara Research for protecting personal data in India. It attempts to bind together ideas on various elements of data protection like definitions, standards, rights, obligations, remedies etc. to present an integrated approach. We recognise our limitations in legislative form and drafting, and welcome feedback and comments on this as a learning document to refine our thinking. Comments welcome at Communications.Research@dvara.com.

- (2) It shall extend to the whole of India, and as provided in this Act, to any offence or contravention of the provisions of this Act committed outside India by any entity.
- (3) It shall come into force on such date as the Central Government may, by notification in the official Gazette, appoint; and different dates may be appointed for different provisions of this Act and any reference in any such provisions to the commencement of this Act shall be construed as a reference to the commencement of that provision.

2. In this Act, unless the context otherwise requires,

- (a) “automated decision-making” is the ability to make or assist in making decisions by technological means;
- (b) “bench” refers to each bench established pursuant to section 23(6)(f) of this Act;
- (c) “breach” means unauthorised access, destruction, use, processing, storage, modification, re-identification, unauthorised disclosure (either accidental, incidental or unlawful) or other reasonably foreseeable risks or data security breaches pertaining to personal data transmitted, stored or otherwise processed;
- (d) “complaints database” means the database established pursuant to section 23(7) of this Act;
- (e) “consent” means the specific, informed and unambiguous acceptance by an individual, who is not under any duress or undue influence of any entity or third party at the time of such acceptance, through clear, affirmative action signifying agreement of the individual to the collection of personal data relating to him or her;

Provided that in the case of an individual who is known or could reasonably be believed to be under 13 years old, it shall refer to the consent of the individual with parental responsibility over the individual whose personal data is sought;

- (f) “data controller” means the natural or legal person which, alone or jointly with others, (1) determines the purposes and means of the processing of personal data or (2) collects personal data from an individual prior to or during the performance or provision of a service or product, or when entering into a contract;

- (g) “data processor” means a natural or legal person which processes personal data on behalf of the data controller;
- (h) “Data Protection Authority” or “Authority” refers to the authority established pursuant to section 22 of this Act;
- (i) “de-identified Information” is information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual;
- (j) “enforcement action” means any action taken by the Data Protection Authority to ensure adherence to the provisions of this Act, including the actions specified in section 23(4)(c) of this Act;
- (k) “entity” is a data controller or data processor, and includes
 - i. any body corporate incorporated under any law for the time being in force in India; or
 - ii. a foreign company within the meaning of section 2(42) of Companies Act, 2013 (No. 18 of 2013);
- (l) “Government” means, save as otherwise provided in this Act, the Central Government and any State Government or State Governments.
- (m) “harm” is actual or potential injury or loss to an individual, whether such injury or loss is economic or non-economic, quantifiable or non-quantifiable;
- (n) “identifiable natural person” is the natural person 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;
- (o) “individual” means any identifiable natural person in India who is the subject of personal data;
- (p) “judicial authority” is the authority established pursuant to section 23(6)(f) of this Act;
- (q) “legitimate purpose” means, with respect to personal data of an individual, the legal, necessary, proportionate and fair use, disclosure and retention of personal data which is:
 - i. limited to what is necessary for performance of a service or provision of a product or at a stage immediately prior to performing the service

or providing a product , and where no less intrusive means are available; or

- ii. required in furtherance of a legal obligation; or
- iii. necessary for administration of justice pursuant to a court order; or
- iv. required for performance of any statutory, governmental or other functions by data processor or data controller as duly specified to the individual subject to data collection; or
- v. necessary to protect the vital interests of the individual or of another individual, particularly where the individual is a child, including but not limited to the case of an individual's medical emergency which is fatal or may likely lead to permanent or irreversible bodily harm; or
- vi. necessary for the third party to whom data is disclosed after it is duly informed to the individual, provided that the interests of data processors or data controller or third parties shall be adequately balanced against any prejudicial effect of the same on the rights and freedoms of the individual as guaranteed under this Act:

Provided that the interests of data processors or data controllers or third parties do not override the interests, rights and freedoms of the individual as provided under the Constitution of India;

- (r) “national identifier” means any form of national identification issued by the Government including an identification number issued to an individual under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (No. 18 of 2016), identification documents or numbers issued under the Passport Act 1967 (No. 15 of 1967), the Representation of People Act, 1950 (No. 43 OF 1951), the Income Tax Act, 1961 (No. 43 of 1961), the Citizenship Act, 1955 (No. 57 of 1955), the Registration of Births and Deaths Act, 1969 (No. 18 of 1969) or any other Act or Scheme of the Government;
- (s) “personal data” means any information that relates to an individual which, either directly or indirectly, including in combination with other information available or likely to be available, is capable of identifying such individual;
- (t) “privacy notice” means the notice given in accordance with section 15(2) of this Act;

- (u) “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, analysis, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- (v) “profiling” means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
- (w) “protected characteristics” include race, gender, ethnic origin, political or religious beliefs, place of birth, caste or indicators when used to identify caste, marital status, age, genetic or health status, sexual orientation and any other characteristics as may be incorporated or defined from time to time by the Government;
- (x) “sensitive personal data” includes such personal data which consists of information relating to or which serves to reveal —
 - i. racial or ethnic origins, political or religious views;
 - ii. passwords;
 - iii. financial information such as bank account or credit card or debit card or other payment instrument details or financial transactions records or other information that would permit access to an account;
 - iv. physical, physiological and mental health condition;
 - v. sexual activity;
 - vi. medical records and history;
 - vii. biometric data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification including, but not limited to, facial images, genetic information, fingerprints, handprints, footprints, iris recognition, handwriting, typing dynamics, gait analysis and speech recognition;
 - viii. any details relating to clauses (i) to (vii) above as provided to body corporates for providing service; and

- ix. any of the information received or collected under clauses (i) to (vii) above by body corporates for processing, stored or processed under lawful contract or otherwise;
- (y) “systemically important data entities” means entities categorised pursuant to section 23(4) of this Act;
- (z) “third party” means a natural or legal person other than the individual, data controller, data processor and natural or legal persons who, under the direct authority of the data controller or data processor, are authorised to process personal data.

3. This Act shall apply to

- (a) all data processing activity, including collection, use, storage, sharing and disclosure of personal data of all individuals through wholly or partially automated or manual methods;
- (b) all entities as defined herein, and such body corporate, incorporated by any Act for the time being in force, as the Central Government may, by notification, specify in this behalf, subject to such exceptions, modifications or adaptation, as may be specified in the notification.

4. This Act shall not apply to

- (a) reasonable safeguards for sovereignty or integrity of India, national security and for the defence of country;
- (b) investigation of cognisable and non-bailable offences under the Indian Penal Code, 1860 (No. 45 of 1860) after a report has been duly filed under section 154 of the Criminal Procedure Code, 1973 (No. 2 of 1974);
- (c) investigation of any other offences under the Indian Penal Code, 1860 (No. 45 of 1860), or any other Act for the time being in force;
- (d) maintenance of public order in situations of imminent danger of breakdown; and
- (e) personal data used for purely personal or household reasons, journalistic, artistic or literary purposes, or of a deceased individual or to any de-identified information.

save that, the provisions of section 18 shall apply to all entities involved in the activities mentioned in this section 4 and **provided that** the exemption in this section

4 must be, reasonable and proportionate, not excessive in nature but satisfy necessary and legitimate purposes, and must be imposed in the manner prescribed.

Chapter II

Individual Privacy Rights and Protections

5. Individual Rights and Protections

- (1) No entity shall collect, store, process, share, disclose or otherwise handle any personal data, intercept any communication of another individual or carry out surveillance of any individual except in accordance with the provisions of this Act and all applicable laws.

6. Rights at Collection and Rights relating to Consent

- (1) For the collection of personal data, consent must be obtained from the individual pursuant to the notice under section 15 of this Act and consistent with such notice.
- (2) Where the purpose of processing of personal data is modified in any material manner, additional data collection or the processing of any personal data previously collected for a different purpose which is in variance with the initial purpose shall not be done without the prior consent of the individual.
- (3) Any entity requesting consent must do so in close proximity to the time of the collection of the personal data, in a manner that is accessible clear, and conspicuous and prominent considering the context in which it is obtained, using clear and plain language taking into account the level of understanding and communications skills of the individuals whose consent is sought.
- (4) Consent, not limited to sub-section (2), shall not be the basis for overriding or reducing protections and limitations, including on using, storing, processing, sharing, disclosure or other handling of personal data, in this Act or any other applicable law.
- (5) Notwithstanding the above, consent may be overridden in cases where there is a legal obligation or medical emergency which is fatal or may likely lead to permanent or irreversible bodily harm, provided that any consent may only be overridden to the extent necessary and, where practicable, the individual so affected shall be informed of the same.

- (6) Entities shall not condition access to services on providing consent unless the personal data is necessary for the provision of services. At any time, an individual shall be entitled to revoke consent and have all personal data collected by the entity returned and deleted, except as otherwise required by law. It shall be as easy to revoke consent as it is to give it.
- (7) Collection of personal data shall only be for legitimate purposes and only the minimum information necessary for such purposes shall be collected.
- (8) With regard to national identifiers,
 - (a) individuals shall not be denied any right, benefit, or privilege because of such individuals' refusal to disclose their national identifier unless necessary for legitimate purposes or otherwise required by law;
 - (b) any entity requesting disclosure of a national identifier shall inform that individual whether:
 - i. such disclosure is mandatory or voluntary
 - ii. the nature of information that may be shared;
 - iii. the uses to which the information received may be put by the requesting entity; and
 - iv. alternatives to submission of the particular national identifier information in question to the requesting entity,
 - (c) such entities shall maintain records of the disclosures sought which may be communicated to the relevant authority issuing the national identifier as required under the law,
 - (d) any entity that collects national identifiers shall be prohibited from using such National Identifier in a manner that provides access to that national identifier by the public, including but not limited to publicly displaying or printing the national identifier on any card used to access products or services provided by the individual.

7. Rights relating to Processing for Legitimate Purposes

- (1) Processing of personal data is only permitted to the extent of the legitimate purposes for which the information was collected as stated in the notice provided.
- (2) At any time, upon notice from the subject of the personal data, or their

representative, entities must cease contacting the individual for solicitation or marketing purposes.

- (3) Any additional or further processing of personal data for archival or scientific or historical or statistical research, shall be considered compatible with the initial purpose if it is,—
 - (a) bona fide;
 - (b) in public interest; and
 - (c) subject to adequate safeguards.

8. Sharing and Access to Personal Data

- (1) Data controllers may share information with other data controllers whose security procedures and privacy policies are no less rigorous and only if consistent with the legitimate purposes for which such information was collected.
- (2) Data controllers may share information with data processors in support of the legitimate purposes for which the information was collected only if the data processor agrees to maintain security procedures and privacy policies no less rigorous than those employed by the data controller.
- (3) If an entity receives a request from a statutory authority for access to personal data, where practicable and if not prohibited by law, the entity shall promptly notify the individual who is the subject of the information to provide that individual with the opportunity to object to disclosure of personal data to the Government or statutory authority or sharing of personal data with the Government or statutory authority.
- (4) If an entity receives a request for access to personal data from a statutory authority, the entity may provide such access if:
 - (a) required by law or court order; or
 - (b) in cases of imminent threats to health and safety.
- (5) An entity may transfer personal data to a successor entity in the same line of business if individuals are provided advance notice of the transfer and the option to have their personal data collected by the entity returned and deleted prior to the transfer.
- (6) Data controllers and data processors shall not disclose personal data to any third party other than as provided in sections 10 of this Act.

9. Rights to Access and Quality of Personal Data

- (1) Every individual shall have the right to seek access to personal data from such individual or generated by or associated with that individual's personal data, which is collected, processed, used or stored by an entity, and such access will be provided:
 - (a) upon proper identification;
 - (b) within a reasonable time not to exceed ten business days;
 - (c) at no charge or a nominal charge;
 - (d) in a reasonable manner, and through a clear user interface that allows them to make informed choices about who sees their data, how it is used, and where and how it is stored;
 - (e) where possible, through the same medium in which the information was provided; and
 - (f) in a form that can be retained and is intelligible to the individual.
- (2) When access to personal data is provided, the individual shall be informed of:
 - (a) The purposes of processing the information;
 - (b) the recipients of such information;
 - (c) whether the individual's national identifier is provided;
 - (d) the period for which such information will be retained;
 - (e) the right to dispute such information and request that it be corrected or erased;
 - (f) the right to lodge a complaint with the Authority;
 - (g) where the information was not collected from the individual, information about the source of the information;
 - (h) the existence of automated decision making and profiling.
- (3) If any individual believes that his or her personal data is inaccurate, untimely or incomplete, or unlawfully collected or processed, he or she shall have the right to have his or her personal data updated, corrected or deleted by the entity.
- (4) Any individual may make an application to an entity to exercise his or her right to have his or her personal data updated, corrected or deleted by the entity.

Provided that

- (a) the entity will have thirty calendar days from receipt of such an application to examine the application, following which the personal data must be updated, corrected or deleted unless the examination of the application confirms the correctness of the current personal data; and

- (b) while a dispute is pending, the entity shall restrict processing of the disputed personal data of the individual; and
 - (c) upon completion of the investigation, if a change results, the entity shall take steps to provide an update to third parties that were provided the personal data prior to or during the dispute.
- (5) Every entity has a duty to take reasonable steps to ensure the accuracy, timeliness and completeness of personal data it holds or controls.
- (6) The individual shall have the right to receive personal data concerning him or her, which he or she has provided to a data controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another specified data controller without hindrance from the data controller to which the personal data have been provided, especially where the processing is carried out by automated means.
- (a) In exercising his or her right to data portability, the individual shall have the right to have the personal data transmitted directly from one data controller to another, where technically feasible and practicable;
 - (b) the right referred to in this subsection shall not adversely affect the rights and freedoms of other individuals.

10. Cross Border Transfers of Personal Data

- (1) Any transfer of personal data outside the territory of India to a foreign country shall take place only if the data controller or data processor has ensured that necessary, reasonable and enforceable safeguards, with effective legal remedies for individuals, are available in the territory of the foreign country such as:
 - (a) the foreign country's level of legal protections;
 - (b) adequate contractual provisions;
 - (c) an agreement between the foreign country and the Central Government or an international agreement to which the Central Government is a party.
- (2) Notwithstanding the foregoing, a transfer of personal data to a third country shall be permitted if:
 - (a) The transfer is necessary for the performance of a contract between the individual and the data controller;
 - (b) necessary in public interest;

- (c) necessary to protect the vital interests of the individual or of other individuals where the individual is physically or legally incapable of giving consent;
- (d) transfer is necessary for the establishment, exercise, or defense of legal claims;
- (e) the personal data is publicly available.

11. Retention of Personal Data

- (1) No personal data shall be retained or kept in a form which permits identification of individuals
 - (a) for longer than necessary after the achievement of legitimate purpose for which it was collected;
 - (b) if obtained unlawfully;
- (2) Notwithstanding anything contained in this section, any personal data may be stored for a period longer than is necessary to achieve the legitimate purpose for which it was collected or received, or, if that legitimate purpose has been achieved or ceases to exist for any reason, for any period following such achievement or cessation, if there are overriding legitimate interests and it is necessary—
 - i. for compliance of a legal obligation or court order or an any action taken by an officer in exercise of the power vested in him or her;
 - ii. for establishing or defending a legal claim;
 - iii. it is required to be stored for legally mandated purposes, such as tax, historical, statistical or research purposes:
 - (i) Provided that only that amount of personal data that is necessary to achieve the purpose of storage under this subsection shall be stored, subject to the implementation of the appropriate technical and organizational measures to safeguard the rights and freedoms of the individuals, and any personal data that is not required to be stored for such purpose shall be destroyed forthwith;
 - (ii) any person who maintains or otherwise possesses personal data for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

12. Rights relating to Automated Decision-making: If an automated tool is used by the entity in whole or part to make decisions regarding an individual, the entity:

- (a) must provide meaningful information to the individual about the basis on which the decision was made at, as well as the significance and envisaged consequences of such processing for the individual;
- (b) has a duty to disclose reasons for decisions;
- (c) demonstrate through a prior assessment that the tool is predictive for a legitimate purpose and non-discriminatory against protected characteristics;
- (d) be subject to data audits by the Authority.

13. Right against Harm:

- (1) Every entity shall make reasonable efforts to ensure that personal data is not used, disclosed or retained in ways that cause harm to individuals.

14. Right to Informational Privacy:

- (1) All individuals shall have a right to informational privacy pursuant to which they shall have the right to prevent information about themselves from being disseminated and to control the extent of access by any entity to their personal data.
- (2) Every entity shall make reasonable efforts to ensure that it accesses and processes personal data in a manner that is consistent with the right to informational privacy of individuals as described in section 14(1).

15. Notice

- (1) Every individual shall be duly informed about the collection and processing of personal data through issuance of a privacy notice as described in section (2) which shall be conspicuous, concise, timely, updated, transparent, intelligible and easily accessible form written in clear, plain and understandable language both in English and predominant language of the individual's geographical area and, where a significant portion of the population has limited literacy skills, in a visual and written format, in a form that can be retained and provided free of cost to the individual.
- (2) Where personal data relating to an individual are collected from the individual, the data controller shall, at the time when personal data are obtained, provide the individual with all of the following information through a privacy notice:

- (a) the identity and the contact details of the data controller and, where applicable, of the data controller's representative;
 - (b) the description of the information collected including from third parties;
 - (c) whether providing the personal data is voluntary or mandatory and the consequences of failure to provide the personal data;
 - (d) the contact information for revoking consent;
 - (e) the legitimate purposes for which the information will be used;
 - (f) to whom the information may be disclosed including transfers of personal data to another country;
 - (g) describing the right of the individual to request access to the information;
 - (h) describing the right of the individual to withdraw the collected information;
 - (i) describing any potential use of automated decision making, and in doing so also be in accordance with section 6(3);
 - (j) indicating where there is a possible transfer of personal data to countries that do not provide adequate legal protection and safeguards for the data;
 - (k) for information collected about the individual from third parties, the notice must also provide information regarding –
 - i. the identity and contact information for such third parties;
 - ii. the purposes of processing that information and the legal basis for such processing;
 - iii. the categories of data;
 - iv. the right to access such information and dispute its accuracy;
 - v. the nature of security measure to protect the information;
 - vi. how long information will be retained.
- (3) If the data controller is making automated decisions, the notice must also –
- (a) inform the individual that the data controller is engaging in this type of activity;
 - (b) provide meaningful information to the individual about the basis on which the decision was made arrived;
 - (c) and explain the significance and envisaged consequences of such automated decision making.
- (4) The Authority is authorised to provide guidance regarding the format and substance of notices, including the publication of model notices.

16. Privacy By Design

- (1) Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing, the data controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures designed to implement data protection principles, including data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Act and protection of the rights of individuals.
- (2) The data controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

17. Data Protection Officer

- (1) Every data controller, data processor or third party shall appoint a Data Protection Officer having adequate technical expertise in the field of data collection or processing and the ability to address any requests, clarifications or complaints made with regard to the provisions of this Act;
- (2) Provided that the data controllers and processors employing less than five hundred people and having an annual turnover of less than one crore rupees may jointly appoint a Data Protection Officer, for resolving or addressing any requests, clarifications or complaints made herein in collaboration with other bodies with similar size or turnover.
- (3) The Data Protection Officer shall:
 - (d) inform and advise the data controller or the data processor pursuant to this Act;
 - (e) monitor compliance with this and with the policies of the data controller or data processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and related audits;
 - (f) cooperate with and act as the contact point for the Authority.

- (g) in the performance of his or her tasks have due regard to the risk associated with processing operations, considering the nature, scope, context and purposes of processing.
- (4) Individuals may contact the Data Protection Officer regarding all issues related to processing of their personal data and to the exercise of their rights under this Act.
- (5) The Data Protection Officer shall be bound by appropriate secrecy or confidentiality obligations concerning the performance of his or her tasks in relation to the handling of personal data.
- (6) The Data Protection Officer may fulfil other tasks and duties. The data controller or data processor shall ensure that any such tasks and duties do not result in a conflict of interests.
- (7) No additional fee shall be charged for resolving or addressing any requests, clarifications or complaints made herein.
- (8) The Data Protection Officer shall—
 - (h) act as an independent person;
 - (i) address requests, clarifications or complaints made in writing, including through electronic form, by any aggrieved individual or legal representative thereof;
 - (j) take steps to initiate an inquiry and commence proceedings within seven days of receiving the complaint;
 - (k) resolve the matter within thirty days of receipt of complaint, and where the matter is not resolvable in this period provide an explanation to the individual making the complaint and the period by which the matter will be resolved which shall not exceed ninety days;
 - (l) recommend the data controller or data processor to take appropriate action; and
 - (m) record the proceedings, the results thereof and the reasons for arriving at the decision in writing.
- (9) In cases where the Data Protection Officer has not been appointed or is unable to or does not adequately resolve the complaints within the stipulated period of ninety days, the complainant may approach the Authority for redressal of complaints.

18. Data Security

- (1) Data controllers, data processors, and entities exempt under section 4, shall take security measures necessary for safeguarding and securing the personal data in their custody with due diligence including:

- (a) designating one or more employees to coordinate their information security program;
 - (b) identifying and assessing the risks to personal data in each relevant area of their operation, and evaluating the effectiveness of the current safeguards for controlling these risks;
 - (c) designing and implementing a safeguards program, and regularly monitoring and testing it;
 - (d) selecting service providers that can maintain appropriate safeguards, making sure their contract requires them to maintain safeguards, and overseeing their handling of customer information; and
 - (e) evaluating and adjusting the program in light of relevant circumstances, including changes in their business or operations, or the results of security testing and monitoring.
 - (f) Data controllers and data processors, where appropriate, shall employ methods for de-identification and encryption of personal data.
- (2) When designing any procedures or systems for handling personal data, data processors and data processors shall address and incorporate any appropriate security measures.

19. Breach Notification

- (1) Every individual shall be promptly informed about any breach involving sensitive personal data that is likely to cause harm,
 - a. **Provided that** it is the duty of the data controller or, on its behalf, the data processor or third party, to provide a breach notification to the individual as soon as possible from the occurrence of the breach as well as take adequate measures to mitigate any harm or damage;
 - b. **Provided further** that in the event that such breach notification is impractical, due to an inability to contact individuals or the substantial number of individuals involved, a breach notification may be made by publication in a manner reasonably likely to clearly and unambiguously put such individuals on notice of the breach,

Save that where a public body responsible for the prevention, detection, or investigation of offences or the Authority determines in writing that such notification will impede a law enforcement investigation or result in other adverse consequences

for public order or safety, the breach notification may be delayed for the period specified in such written determination.

- (2) The burden of proof to substantiate that adequate measures have been taken in accordance with the provisions of this Act, shall lie on the data controller or data processor or third party.
- (3) The breach notification provided under this section as specified by the Data Protection Authority shall include:
 - (a) the identity of the data controller, even in cases where the notice is provided by the data processor or a third party;
 - (b) a general description of the breach;
 - (c) the types of information compromised and the likely consequences of the breach;
 - (d) the estimated date or range of dates of the breach;
 - (e) the number of individuals involved;
 - (f) the steps taken to mitigate and remediate the breach;
 - (g) the rights available to individuals and the contact information of the entity providing the notice.
- (4) The data controller or data processor, on its behalf, shall notify the Authority any time such notice has been provided. The notice to the Authority shall state:
 - (a) The nature of the breach
 - (b) The systems affected
 - (c) The number of individuals whose data was compromised
 - (d) The remedial actions taken.
- (5) Every breach must be notified to the Data Protection Authority.
- (6) The Authority shall establish and maintain a public registry of breach notifications received from data controllers and data processors and publish all notices received on the registry.

20. Liability of entities:

Any entity that fails to collect, store, process, disclose, use, share or otherwise handle any personal data in accordance with the terms of this Act shall be liable in respect of the violation of any of the rights provided under this Act as a result of such failure,

Provided that where multiple entities are responsible for a failure under this provision, their liability shall be joint and several.

Provided further that, such entity shall be given a reasonable opportunity of being heard before the judicial authority before any penalty is imposed.

21. Burden of Proof:

Where an individual establishes *prima facie* that an entity's act or omission has resulted in a violation of any of such individual's rights provided under this Act, the burden of proof shall lie on the entity to prove that it did not commit or was not responsible for the commission of the acts or omissions in question.

CHAPTER III

Powers and Functions of the Data Protection Authority

22. The Data Protection Authority

- (1) The Data Protection Authority shall be constituted to undertake the functions and fulfill the regulatory objectives specified in this Act.
- (2) The Central Government shall, by notification in the Official Gazette, and in consultation with the Chief Justice of India, appoint a Chairperson and other members to the Data Protection Authority in such manner as may be prescribed.
- (3) Regulatory Objectives: The Data Protection Authority shall carry out its functions in furtherance of the objectives in the Preamble to this Act.
- (4) Relationship with the Cyber Appellate Tribunal²
 - (a) Appeals from orders of the judicial authority shall be made to the Cyber Appellate Tribunal constituted under Information Technology Act 2000 (as amended);
 - (b) The Data Protection Authority shall have the authority to monitor compliance with the orders of the Cyber Appellate Tribunal, where such orders relate to appeals from the orders of the judicial authority.

² We note that following the Finance Act of 2017, the Cyber Appellate Tribunal under the Information Technology Act was collapsed and the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) took over its mandate. However, a telecom appellate authority would not be an appropriate forum to consider the wide-ranging appeals that will arise in the broad field of data protection. Rather than using the TDSAT, a potential solution could be to refurbish the Cyber Appellate Tribunal structure and have its capacity strengthened, so that it can be a relevant appellate body for issues of data protection.

23. Powers and Functions of the Data Protection Authority

- (1) **Directions:** The Data Protection Authority may, for the discharge of its functions under the provisions of this Act, issue such directions from time to time, as it may consider necessary.
- (2) **Advice:** The Data Protection Authority may provide advice to other government agencies, entities or individuals regarding any matters within its jurisdiction as well as public and business education.
- (3) **Monitoring and research:** The Data Protection Authority shall monitor cross-border transfers of data and security breaches exclusively for research purposes and engage in research regarding the collection, use, disclosure and retention of personal data.
- (4) **Supervision and enforcement:** The Data Protection Authority shall ensure compliance with the provisions of this Act and any rules made under this Act, including by undertaking enforcement actions in accordance with the provisions of this section 23(4)(c) of this Act.
 - (a) The Data Protection Authority shall promulgate rules regarding its supervisory activities:
 - i. by developing a methodology comprising both quantitative and qualitative indicators according to which the entities processing personal data may be categorised as:
 - (1) systemically important data entities,
 - (2) normal risk entities, and
 - (3) low risk entities.
 - ii. on the types of enhanced supervisory activities undertaken by the Data Protection Authority based on an entity's categorisation as a systemically important data entity including, but not limited to:
 - (1) increased frequency and depth of supervisory activities;
 - (2) review of disaster recovery and resolution plans which may be mandated;
 - (3) Increased reporting obligations to the Data Protection Authority; or
 - (4) periodic audits in connection with data security.
 - iii. to allow for inter-sectoral coordination with relevant public authorities and sectoral regulators to operationalise supervisory arrangements with

regard to entities processing personal data that are not systemically important data entities.

(b) The Data Protection Authority,

- i. may undertake enforcement actions on its own initiative, on the basis of complaints, including on the basis of information received from the scrutiny of the complaints database, and on the basis of referrals from other public authorities or government agencies; and
- ii. shall undertake enforcement actions where information received from the scrutiny of the complaints database provide reasonable cause to suspect contravention, or the likelihood of contravention, of any provisions of this Act or any order or direction issued by the Data Protection Authority under this Act

(c) The Data Protection Authority may undertake such enforcement actions as required to fulfill its mandate under sub-section (4)(a) including through the:

- i. issuance of a private warning;
- ii. issuance of informal guidance in response to a clarification sought by any individual or entity;
- iii. issuance of a public statement
- iv. issuance of a show cause notice;
- v. launching of an investigation in accordance with this section 23(4)(g) of this Act;
- vi. issuance of a direction requiring any individual or entity to remedy any contravention of the provisions of this Act, or any order or direction issued by the Data Protection Authority under this Act, including, but not limited to, compensation taking into account the amount of unfair advantage as a result of such contravention, the amount of harm to any individual, and the repetitive nature of the default;
- vii. monitoring compliance with the orders of the Cyber Appellate Tribunal, where such orders relate to appeals from the orders of the judicial authority;
- viii. imposition of a monetary penalty the amount of which shall take into account the degree of culpability, any history of prior such conduct, ability to pay, effect on ability to continue to do business, and such other matters as justice may require;

- ix. recommendation to relevant public authorities and sectoral regulators to take such steps as they may be empowered to with respect to any particular individual or entity;
- (d) Any enforcement action authorised by the Data Protection Authority must be proportionate to the contravention of the provision of this Act, or any order or direction issued by the Data Protection Authority under this Act, in respect of which such an enforcement action is authorized;
- (e) The Data Protection Authority must consider the following factors while determining the enforcement action to be taken against an entity:
 - i. the nature and seriousness of the contravention of the provisions of this Act, or any order or direction issued by the Data Protection Authority under this Act, by the entity,
 - ii. the consequences and impact of the contravention of the provisions of this Act, or any order or direction issued by the Data Protection Authority under this Act, including the extent of,
 - (1) benefit or unfair advantage gained by the entity as a result of the contravention; and
 - (2) loss and harm caused, or likely to be caused, to individuals as a result of the contravention;
 - (3) repetitive or continuing nature of the contravention default prior to the enforcement actions; and
 - (4) other contraventions committed by the entity under this Act.
- (f) An enforcement action by the Data Protection Authority for a contravention of the provisions of this Act, or any order or direction issued by the Data Protection Authority under this Act, does not bar the Data Protection Authority from prosecuting an entity for an offence under this Act, but any fine required to be paid upon conviction for an offence may be set off against any monetary penalty paid by such entity in an enforcement action in respect of the same cause of action.
- (g) Where the Data Protection Authority has information or reasonable grounds to suspect that any entity is in contravention of the provisions of this Act, or any order or direction issued by the Data Protection Authority under this Act, it may investigate such contravention by:

- i. appointing one or more investigators to investigate the contravention; and
 - ii. recording such appointment by providing
 - (1) the appointment of the investigator;
 - (2) reason for commencing the investigation;
 - (3) scope of the investigation;
 - (4) the duration of the investigation, which will not exceed one hundred and eighty days in the first instance; and
 - (5) the method of reporting of the investigation provided that the Data Protection Authority may modify the terms of appointment, if the circumstances of the investigation require such modification.
- (h) The investigator appointed pursuant to this section 23(4) of this Act will have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, including in respect of the following matters, namely:
- i. the discovery and production of any document, including books of account or other documents showing compliance with the provisions of this Act;
 - ii. summoning and enforcing the attendance of any natural person and examining them on oath;
 - iii. requiring such natural persons to produce relevant records and documents; and
 - iv. issuing commissions for the examination of natural persons or documents.
- (5) **Inter-sectoral coordination:** The Data Protection Authority shall take steps to ensure coordination between relevant public authorities and sectoral regulators, in accordance with the provisions of this section 23 of this Act.
- (a) In discharging its functions under this Act, the Data Protection Authority will coordinate with relevant public authorities and sectoral regulators, including telecom authorities, financial sector authorities, health authorities, the Unique Identification Authority of India and others as appropriate in order to:
- i. request for information from the other authorities in respect of investigations in progress or in connection with enforcement actions;

- ii. to receive references or notifications from other authorities of the contravention of the provisions of this Act, or to make available to other authorities any order or direction issued by the Data Protection Authority under this Act, with regard to entities regulated by them;
- iii. to issue and enforce enforcement actions under this Act;
- iv. to recommend enforcement actions to be undertaken by the other authorities;
- v. to make rules for the coordination between authorities as required pursuant to this provision of this Act, including formation of memorandums of understanding between authorities in furtherance of this objective.

(6) Adjudication:

- (a) The Central Government shall, by notification in the official Gazette, establish a judicial authority to adjudicate all disputes and contraventions of the provisions of this Act.
- (b) The judicial authority shall consist of a Chairperson and not more than two Members to be appointed, by notification in the official Gazette, by the Central Government.
- (c) The selection of Chairperson of the judicial authority shall be made by the Central Government in consultation with the Chief Justice of India.
- (d) The selection of the Members of the judicial authority shall be made by the Central Government in consultation with the Chairperson.
- (e) The judicial authority shall consist of at least one judicial and one technical Member,
 - i. A judicial Member shall otherwise be qualified to be a High Court Judge or have been a member of the Indian Legal Services and have held a post in Grade I of that Service for at least three years.
 - ii. A technical Member shall have expertise, special knowledge of and adequate professional experience in technology and processing/collection of data.
- (f) Subject to the provisions of this Act,
 - i. the jurisdiction of the judicial authority may be exercised by the any benches constituted thereof.

- ii. The judicial authority shall comprise such benches as the Central Government may, in consultation with the Chairperson, by notification in the Official Gazette, specify.
- iii. A bench may be constituted by the Chairperson of the judicial authority with one or two Members of such judicial authority as the Chairperson may deem fit.
- iv. The Central Government shall, by notification in the Official Gazette, specify the areas in relation to which each bench of the judicial authority may exercise its territorial jurisdiction.

(7) Procedure and powers of the judicial authority:

- (a) The judicial authority shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908) but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the judicial authority shall have powers to regulate its own procedure including the place at which it shall have its sittings.
- (b) The judicial authority shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely:—
 - i. summoning and enforcing the attendance of any natural person and examining him on oath;
 - ii. requiring the discovery and production of documents or other electronic records;
 - iii. receiving evidence on affidavits;
 - iv. issuing commissions for the examination of witnesses or documents;
 - v. reviewing its decisions;
 - vi. dismissing an application for default or deciding it ex parte;
 - vii. any other matter which may be prescribed.

(8) Appeal to Supreme Court

- (a) Notwithstanding anything contained in the Code of Civil Procedure, 1908 (5 of 1908) or in any other law, an appeal shall lie against any order, not being an interlocutory order, of the Cyber Appellate Tribunal to the Supreme Court on one or more of the grounds specified in section 100 of that Code.

- (b) No appeal shall lie against any decision or order made by the Cyber Appellate Tribunal without the consent of the parties.
- (c) Every appeal under this section shall be preferred within a period of ninety days from the date of the decision or order appealed against: PROVIDED that the Supreme Court of India may entertain the appeal after the expiry of the said period of ninety days, if it is satisfied that the appellant was prevented by sufficient cause from preferring the appeal in time

(9) Redressal:

- (a) Where a complaint made by an individual to an entity pursuant to their rights under this Act has not been resolved within the stipulated period , the individual may bring a complaint against the relevant entity through online lodging, toll-free calling lines, e-mail, letter, fax or in person to the Data Protection Authority if:
 - i. the matter is not pending before, or has not been adjudicated upon by, another competent authority; or
 - ii. the complaint is prima facie not frivolous, malicious or vexatious.

Provided that the complaints shall be received, recorded and tracked by the Data Protection Authority within a complaints database.

- (b) Following the receipt of the complaint, the Data Protection Authority shall:
 - i. promptly send a notice to the relevant entity seeking reasons for the delay in the resolution of the complaint; and
 - ii. upon failure to receive an adequate response from the relevant entity within fifteen business days, take such enforcement actions against the relevant entity pursuant to the Supervision and Enforcement powers under section 23(4) of this Act; and
 - iii. provide prompt notification to the individual of the steps taken under this provision using such modes of communication as used to receive the complaint.

(10) Reporting: The Data Protection Authority shall release a report providing aggregate details:

- (a) every month, on the complaints received including the number, nature, category, geography, sector and such other factors relating to the complaint as appropriate; and
- (b) annually, on the enforcement actions undertaken and complaints acted upon using a format stipulated by the Authority, including such qualitative commentary as it sees fit.

(11) **Meetings:**

- (a) The Data Protection Authority shall meet at such times and places, and shall observe such rules of procedure in regard to the transaction of business at its meetings (including quorum at such meetings) as may be provided by regulations.
- (b) The Chairperson or, if for any reason, he is unable to attend a meeting of the Authority, any other member chosen by the members present from amongst themselves at the meeting shall preside at the meeting.
- (c) The Data Protection Authority may make regulations for the transaction of business at its meetings

CHAPTER IV

Miscellaneous

24. Act not in derogation of any other law: The provisions of this Act shall be in addition to, and not in derogation of, the provisions of any other law for the time being in force.

25. Power to make rules:

- (1) The Central Government may, by notification, make rules for carrying out the purposes of this Act.
- (2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely,
 - (a) the salary and allowances payable to and the other conditions of service of the Chairperson of the Data Protection Authority and members appointed pursuant to this Act;

- (b) the powers and functions of the Chairperson of the Data Protection Authority under this Act;
- (c) The procedure for conducting an inquiry made under section 23 of this Act;
- (d) the salary and allowances and other conditions of service of officers and other employees of the Data Protection Authority;
- (e) the salary and allowances payable to and other terms and conditions of service of the Chairperson and other Members of the judicial authority established pursuant to this Act;
- (f) the salary and allowances and other conditions of service of the officers and employees of the judicial authority;
- (g) any other matter which is to be, or may be, prescribed, or in respect of which provision is to be made, by rules.

26. Delegation: The Data Protection Authority may, by general or special order in writing, delegate to any Member, officer of the Data Protection Authority or any other person, subject to such conditions, if any, as may be specified in the order, such of its powers and functions under this Act (except the power under section 27) as it may deem necessary.

27. Power to make regulations:

- (1) The Data Protection Authority may, by notification, make regulations consistent with this Act and the rules made thereunder to carry out the purposes 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, namely
 - (a) the times and places of meetings of the Authority and the procedure to be followed at such meetings, including quorum necessary for the transaction of business;
 - (b) the transaction of business at the meetings of the Authority under sub-section.

28. Rules and regulations to be laid before Parliament: Every rule and every regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry

of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or regulation or both Houses agree that the rule or regulation should not be made, the rule or regulation shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule or regulation.

29. Power to remove difficulties:

(1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order, published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to be necessary for removing the difficulty:

Provided that no such order shall be made under this section after the expiry of three years from the commencement of this Act.

(2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

Dr. Shashi Tharoor's official website

28/July/2017

THE DATA PRIVACY AND PROTECTION BILL, 2017

A

BILL

to establish an effective regime to protect the right to privacy of all natural persons and personal data concerning them, to set out conditions upon which surveillance of natural persons and interception of communications may be carried out, to constitute a Privacy Commission, and for matters connected therewith and incidental thereto.

WHEREAS the right to privacy is an inalienable right of all persons;

AND WHEREAS the need to protect privacy has only increased in the digital age, with the emergence of big data analytics;

AND WHEREAS the delivery of goods and provision of services requires the collection, storage, processing and disclosure, including international transfers, of personal data;

AND WHEREAS good governance requires that all interceptions of communications and surveillance must be conducted in a systematic and transparent manner subservient to the rule of law;

AND WHEREAS it is necessary to harmonise any conflicting interests and competing legislation;

NOW, THEREFORE, it is expedient to provide for an enforceable means to protect the privacy of persons.

BE IT ENACTED by Parliament in the Sixty-Eighth Year of the Republic of India as follows –

CHAPTER I

Preliminary

1. Short title, extent and commencement. –

- (1) This Act may be called the Data Privacy And Protection Act, 2017.
- (2) It extends to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention hereunder committed outside India by any person.
- (3) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint.

2. Definitions. –

- (1) In this Act and in any rules made thereunder, unless the context otherwise requires, –
- (a) “anonymise” means, in relation to personal data, the encryption or removal of all data that may, whether directly or indirectly in conjunction with any other data, be used to identify a natural person or data subject;
 - (b) “appropriate government” means, in relation to the Central Government or a Union Territory Administration, to the Central Government; in relation a State Government, that State Government; and, in relation to a public authority which is established, constituted, owned, controlled or substantially financed by funds provided directly or indirectly :
 - (i) by the Central Government or a Union Territory Administration, the Central Government;
 - (ii) by a State Government, that State Government;
 - (c) “armed force” means any body raised or constituted pursuant to or in connection with, or presently governed by, the Army Act, 1950 (46 of 1950), the Indian Reserve Forces Act, 1888 (4 of 1888), the Territorial Army Act, 1948 (6 of 1948), the Navy Act, 1957 (62 of 1957), the Air Force Act, 1950 (45 of 1950), the Reserve and Auxiliary Air Forces Act, 1952 (62 of 1952), the Coast Guard Act, 1978 (30 of 1978) or the Assam Rifles Act, 2006 (47 of 2006);
 - (d) “authorised officer” means an officer, not below the rank of a Gazetted Officer, of an All India Service or a Central Civil Service, as the case may be, who is empowered by the Central Government, by notification in the Official Gazette, to intercept a communication of another person or carry out surveillance of another person under this Act;
 - (e) “biometric data” means any data relating to the physical, physiological or behavioural characteristics of a natural person which allow their unique identification including, but not restricted to, facial images, fingerprints, hand prints, foot prints, iris recognition, hand writing, typing dynamics, gait analysis and speech recognition;
 - (f) “Chief Privacy Commissioner” and “Privacy Commissioner” mean the Chief Privacy Commissioner and Privacy Commissioner appointed under section 33;
 - (g) “collect”, with its grammatical variations and cognate expressions, means, in relation to personal data, any action or activity that results in a data controller, police force, armed force, intelligence organisation, public authority, company, person, State or other entity (natural or otherwise) obtaining, or coming into the knowledge or possession of, any personal data of another person;
 - (h) “communication” means a word, signs, gestures, spoken, written or indicated, in any form, manner or language, encrypted or unencrypted, meaningful or otherwise, and includes visual representations of words, ideas, symbols and images, and the meta data in relation whether transmitted or not transmitted and, if transmitted, irrespective of the medium of transmission;

- (i) “competent organisation” means an organisation or public authority listed in the Schedule to this Act;
 - (j) “consent” means an unambiguous indication of a data subject’s agreement to the collection, processing, use or dissemination of personal data relating to him or her.
 - (k) “data controller” means a person who, either alone, or jointly, or in concert with other persons, determines the purposes for which and the manner in which any personal data is processed;
 - (l) “data processor” means a person who processes any personal data on behalf of a data controller;
 - (m) “data subject” means a natural person who is the subject of personal data;
 - (n) “deoxyribonucleic acid data” means all data, of whatever type, concerning the characteristics of a natural person that are inherited or acquired during early prenatal development;
 - (o) “destroy”, with its grammatical variations and cognate expressions, means, in relation to personal data, to cease the existence of, by deletion, erasure or otherwise, any personal data;
 - (p) “disclose”, with its grammatical variations and cognate expressions, means, in relation to personal data, any action or activity that results in a person coming into the knowledge or possession of any personal data of another person;
 - (q) “intelligence organisation” means an intelligence organisation under the Intelligence Organisations (Restriction of Rights) Act, 1985 (58 of 1985) and includes the National Investigation Agency constituted under sub-section (1) of section 3 of the National Investigation Agency Act, 2008 (34 of 2008) and the Central Bureau of Investigation constituted under the Delhi Special Police Establishment Act, 1946;
 - (r) “interception” or “intercept” means any activity intended to capture, read, listen to or understand the communication of a person;
 - (s) “officer-in-charge of a police station” shall have the meaning ascribed to it under clause (o) of section 2 of the Code of Criminal Procedure, 1973 (2 of 1974);
 - (t) “person” means and includes a natural person, a company, a firm, an association of persons or a body of individuals, whether incorporated or not;
 - (u) “personal data” means any data which relates to a natural person if that person can, whether directly or indirectly in conjunction with any other data, be identified from it and includes sensitive personal data;
- Provided that the term “personal data” shall not include data which is a matter of public record except details of victims in cases of sexual assault, kidnapping or abduction.
- (v) “police force” means –

- (i) any body raised or constituted by the appropriate government for the preservation of law and order and enforcement of laws related to customs, revenue, foreign exchange, excise, income tax and narcotics;
 - (ii) the bodies raised or constituted pursuant to or in connection with, or presently governed by, the Police Act, 1861 (5 of 1861), the Central Reserve Police Force Act, 1949 (66 of 1949), the Border Security Force Act, 1968 (47 of 1968), the Indo-Tibetan Border Police Force Act, 1992 (35 of 1992), the Sashastra Seema Bal Act, 2007 (53 of 2007), the Central Industrial Security Force Act, 1968 (50 of 1968), the Railway Protection Force Act, 1957 (23 of 1957) and the National Security Guard Act, 1986 (47 of 1986);
 - (iii) the bodies raised or constituted pursuant to or in connection with, or presently governed by, the Delhi Special Police Establishment Act, 1946 (25 of 1946), the Income Tax Act, 1961 (43 of 1961), the National Investigation Agency Act, 2008 (34 of 2008) and the Central Vigilance Commission Act, 2003 (45 of 2003);
 - (iv) any police forces raised or constituted by the States, armed or otherwise;
- (w) “prescribed” means prescribed by rules made under this Act;
- (x) “Privacy Commission” means the Privacy Commission constituted under sub-section (1) of section 33;
- (y) “Privacy Officer” means the Privacy Officer designated under sub-section (3) of section 22 and sub-sections (3) and (4) of section 30.
- (z) “process”, with its grammatical variations and cognate expressions, means, in relation to personal data, any action or operation which is performed upon personal data of another person, whether or not by automated means including, but not restricted to, organisation, structuring, adaptation, modification, retrieval, consultation, use, alignment or destruction;
- (aa) “public authority” shall have the meaning ascribed to it under clause (h) of section 2 of the Right to Information Act, 2005 (22 of 2005);
 - (bb) “receive”, with its grammatical variations and cognate expressions, means, in relation to personal data, to come into the knowledge or possession of any personal data of another person;
 - (cc) “sensitive personal data” means personal data or metadata as to a person’s
 -
 - (i) biometric data;
 - (ii) deoxyribonucleic acid data;
 - (iii) sexual preferences and practices;
 - (iv) medical history and health;
 - (v) political affiliation;

- (vi) ethnicity, religion, race or caste; and
 - (vii) financial and credit information, including financial history and transactions.
- (dd) “store”, with its grammatical variations and cognate expressions, means, in relation to personal data, to retain, in any form or manner and for any purpose or reason, any personal data of another person;
- (ee) “surveillance” means any activity, directly or indirectly intended to watch, monitor, record or collect, or to enhance the ability to watch, record or collect, any information, images, signals, data, movement, behaviour or actions, of a person, a group of persons, a place or an object, for the purpose of obtaining information of a person, but does not include collection of personal data under Sections 7 and 8 of this Act;
- (2) All other expressions used herein shall have the meanings ascribed to them under the General Clauses Act, 1897 (10 of 1897) or the Code of Criminal Procedure, 1973 (2 of 1974), as the case may be.

3. Principles applicable to protecting privacy. – In exercising the powers conferred by this Act, regard shall be had to the following considerations, namely –

- (a) that personal data with its attributes belongs solely to the person to whom it pertains;
- (b) that personal data is required by governments and commercial service providers and others to enable good governance and the delivery of goods and provision of services without undue delay which may be provided by a meaningful, revocable notice and consent framework;
- (c) that the right to privacy is recognised as a fundamental human right by various international treaties to which India is a party;
- (d) that intrusions into privacy need always be measured by principles of necessity and proportionality;
- (e) that the right to privacy is a fundamental right essential to the maintenance of a democratic society;
- (f) that privacy must be upheld by a competent authority that is independent, impartial, well resourced and free from unwarranted influence.

CHAPTER II

Right to Privacy

4. Right to privacy. –

- (1) Without prejudice to the generality of the provisions contained herein, all natural persons shall have a right to privacy which shall be implemented as per Section 3 of this Act.

(2) For the purpose of sub-section (1) no person shall collect, store, process, disclose or otherwise handle any personal data of a natural person, intercept any communication of another person, or carry out surveillance of another person except in accordance with the provisions of this Act.

5. Exemptions. – Nothing in this Act shall apply to –

(a) the collection, storage or processing by a person of their own personal data for personal or family use; or

(b) surveillance by a resident of their own residential property.

CHAPTER III

Protection of Personal Data

6. Effecting consent from a data subject –

A data subject may be said to have given effective consent only when -

(1) it is free, in the terms of section 14 of the Indian Contract Act, 1872;

(2) it is obtained prior to all data collection, except in the cases expressly excluded by section 8;

(3) it is voluntarily given through an express and affirmative act and is recorded in writing;

Provided that effective consent can only be said to have been obtained where:

(i) a conspicuous means for its withdrawal is made available to the data subject, and

(ii) the means for its withdrawal can be employed with the same ease as the means by which it was obtained.

(4) it is obtained after the data subject has been duly informed, in language that a reasonable person can comprehend, of the matters enumerated in sub-section (3) of section 7 or sub-section (3) of section 13 as the case may be, and;

Provided that, in case of any dispute, ambiguities in the terms of the notice and of any privacy policies that apply will be resolved in favour of the data subject.

(5) it is specific and limited as to purpose and duration.

Explanation 1: Consent will be deemed to be limited only if it is obtained in respect of the purposes and duration strictly necessary to provide the product or service in relation to which personal data is sought to be collected, processed or disclosed

Explanation 2: When the purposes for which personal data was collected are materially altered or expanded subsequent to its collection, consent will be deemed to be specific only if it is obtained afresh in respect of that alteration or expansion -

- (i) after duly informing the data subject of the alteration or expansion in purpose, and
- (ii) prior to any use of that data for the expanded purposes.

7. Collection of personal data. –

(1) No person, including a data controller and data processor, shall collect any personal data without obtaining the effective consent of the data subject to whom it pertains.

(2) Subject to sub-section (1), no person shall collect any personal data that is not necessary for the achievement of a purpose that is connected to a stated function of the person seeking its collection.

(3) A person seeking to collect any personal data shall, prior to its collection and as notified by the Privacy Commission, inform the data subject free of any charges, direct or indirect, to whom it pertains of the following details in respect of their personal data, namely –

- (a) when it will be collected;
- (b) its content and nature;
- (c) the purpose of its collection;
- (d) the purpose and manner in which it will be used;
- (e) the persons to whom it will be made available;
- (f) the duration for which it will be stored;
- (g) the manner in which it may be accessed, checked and modified;
- (h) the security practices and other safeguards, if any, to which it will be subject;
- (i) whether, and the conditions and procedure upon which, it may be disclosed to others;
- (j) the time and manner in which it will be destroyed, or the criteria used to determine that time period;
- (k) the procedure for recourse in case of any grievance in relation to it; and
- (l) the identity and contact details of the data collector and data processor

(4) Personal data collected in pursuance of a grant of consent by the data subject to whom it pertains shall, if that consent is subsequently withdrawn for any reason, be destroyed forthwith:

Provided that the person who collected the personal data in respect of which consent is subsequently withdrawn may, only if the personal data is necessary for the delivery of any good or the provision of any service, or the fulfilment of a lawful contract, not deliver that good or deny that service or fulfil that contract

to the data subject who withdrew the grant of consent easily and at any point during the duration of a service.

8. Collection of personal data without prior consent. –

Personal data may be collected without the prior consent of the data subject if it is –

- (a) necessary for the provision of an emergency medical service to the data subject;
- (b) required for the establishment of the identity of the data subject and the collection is authorised by a law in this regard;
- (c) necessary to prevent, investigate or prosecute a cognisable offence.

9. Storage and destruction of personal data. –

(1) No person, including a data controller and a data processor, shall store any personal data for a period longer than is necessary to achieve the purpose for which it was collected or received, or, if that purpose is achieved or ceases to exist for any reason, for any period following such achievement or cessation.

(2) Save as provided in sub-section (3), any personal data collected or received in relation to the achievement of a purpose shall, if that purpose is achieved or ceases to exist for any reason, be destroyed forthwith.

(3) Notwithstanding anything contained in this section, any personal data may be stored for a period longer than is necessary to achieve the purpose for which it was collected or received, or, if that purpose has been achieved or ceases to exist for any reason, for any period following such achievement or cessation, if –

- (a) the data subject to whom it pertains grants their effective consent to such storage prior to the purpose for which it was collected or received being achieved or ceasing to exist;
- (b) it is adduced for an evidentiary purpose in a legal proceeding; or
- (c) it is required to be stored for historical, statistical or research purposes under the provisions of an Act of Parliament:

Provided that only such amount of personal data that is necessary to achieve the purpose of storage under this sub-section shall be stored and any personal data that is not required to be stored for such purpose shall be destroyed forthwith:

Provided further that any personal data stored under this sub-section shall, to the extent possible, be anonymised.

10. Processing of personal data. –

(1) No person shall process any personal data that is not necessary for the achievement of the purpose for which it was collected or received.

(2) Save as provided in sub-section (3), no personal data shall be processed for any purpose other than the purpose for which it was collected or received.

(3) Notwithstanding anything contained in this section, any personal data may be processed for a purpose other than the purpose for which it was collected or received if the data subject grants their effective consent to such processing and only that amount of personal data that is necessary to achieve the other purpose is processed.

(4) Notwithstanding anything contained in this section, any personal data may be processed for a purpose other than the purpose for which it was collected or received if –

(a) the data subject grants his/her effective consent to the processing and only that amount of personal data that is necessary to achieve the other purpose is processed;

(b) it is necessary to perform a contractual duty to the data subject;

(c) it is necessary to prevent a reasonable threat to security of the State or public order; or

(d) it is necessary to prevent, investigate or prosecute a cognisable offence.

11. Security of personal data and duty of confidentiality. –

(1) No person shall collect, receive, store, process or otherwise handle any personal data without implementing measures, including, but not restricted to, technological, physical and administrative measures, adequate to secure its confidentiality, secrecy, integrity and safety, including from theft, loss, damage or destruction.

(2) Any person who collects, receives, stores, processes or otherwise handles any personal data shall be subject to a duty of confidentiality and secrecy in respect of it.

(3) Data controllers and data processors shall be subject to a duty of confidentiality and secrecy in respect of personal data in their possession or control.

(4) Without prejudice to the provisions of this section, any person who collects, receives, stores, processes or otherwise handles any personal data shall, if its confidentiality, secrecy, integrity or safety is violated by theft, loss, negligence, damage or destruction, or as a result of any collection, processing or disclosure contrary to the provisions of this Act, or for any other reason whatsoever, as soon as he or she becomes aware of such violation, notify the person to whom it pertains, the Privacy Commission and any other agencies whom the Central Government notifies for this purpose, in such form and manner as may be prescribed, forthwith. Further, any persons, who collects, receives, stores, processes, or otherwise handles any personal data shall report all breaches of provisions of this Chapter III to the Privacy Commission, that are brought to its notice, or are reasonably expected to be known to such persons.

12. Transfer of personal data for processing. –

- (1) Subject to the provisions of this section, personal data that has been collected in conformity with this Act may be transferred by a data controller to a data processor, whether located in India or otherwise, if the transfer is pursuant to an agreement that explicitly binds the data processor to same or stronger measures in respect of the storage, processing, destruction, disclosure and other handling of the personal data as are contained in this Act.
- (2) No data processor shall process any personal data transferred under this section except to achieve the purpose for which it was collected.
- (3) A data controller that transfers personal data under this section shall remain liable to the data subject for the actions of the data processor.

13. Disclosure of personal data. –

- (1) Save as provided in this section, no person shall disclose, or otherwise cause any other person to receive, the content or nature of any personal data, including any other details in respect thereof, except to the person to whom it pertains.
- (2) No person shall disclose any personal data without obtaining the prior effective consent of the data subject and such effective consent may be obtained in any manner, and through any medium, but shall not be obtained as a result of a threat, duress, denial of service or coercion.
- (3) For the purpose of sub-section (2), a person seeking to disclose any personal data shall, prior to its disclosure, inform the data subject of the following details in respect of their personal data, namely: –
 - (a) when it will be disclosed;
 - (b) the purpose of its disclosure;
 - (c) the security practices and other safeguards, if any, to which it will be subject;
 - (d) the privacy policies and other policies, if any, that will protect it; and
 - (e) the procedure for recourse in case of any grievance in relation to it.
- (4) Notwithstanding anything contained in this section, any person who collects, receives, stores, processes or otherwise handles any personal data may disclose it to a person other than the data subject, whether located in India or otherwise, for the purpose only of processing it to achieve the purpose for which it was collected if such a disclosure is pursuant to an agreement that explicitly binds the person receiving it to same or stronger measures in respect of its storage, processing, destruction, disclosure or other handling as are contained in this Act.

14. Quality and accuracy of personal data. –

- (1) Any person who collects, receives, stores, processes or otherwise handles any personal data shall, to the extent possible, ensure that it is accurate and, where necessary, is kept up to date.

(2) No person who collects, receives, stores, processes or otherwise handles any personal data shall deny, to the data subject, the opportunity to review and obtain a copy of such data and, where necessary, rectify anything that is inaccurate or not up to date.

(3) Any person to whom any personal data collected, received, stored, processed or otherwise handled under this Act pertains may, if it is not necessary to achieve the purpose of its collection, reception, storage, processing or other handling, demand its destruction, and the person so collecting, receiving, storing, processing or otherwise handling that personal data shall destroy it forthwith.

15. Special provisions for sensitive personal data. –

Notwithstanding anything contained in this Act and the provisions of any other law for the time being in force –

- (a) no person shall collect sensitive personal data without explicit effective consent from the data subject;
- (b) no person shall store sensitive personal data for a period longer than is necessary to achieve the purpose for which it was collected or received, or, if that purpose has been achieved or ceases to exist for any reason, for any period following such achievement or cessation;
- (c) no person shall process sensitive personal data for a purpose other than the purpose for which it was collected or received;
- (d) no person shall disclose sensitive personal data to another person, or otherwise cause any other person to come into the knowledge or possession of, the content or nature of any sensitive personal data, including any other details in respect thereof, except the data subject.

16. Special provisions for intelligence organisations. –

(1) Notwithstanding anything contained in this Act, the provisions of section 6, section 7, section 8, sub-section (4) of section 10 and section 11 shall not apply in respect of an intelligence organisation.

(2) Any intelligence organisation seeking to collect any personal data shall prefer an application, in such form and manner as may be prescribed, to the Chief Privacy Commissioner or any other person authorised by him in this behalf.

(3) The Chief Privacy Commissioner, or any other person authorised by him in this behalf, may, if he is satisfied that the collection of the personal data is necessary to prevent a reasonable threat to security of the state or public order, or prevent, investigate or prosecute a cognisable offence, order the collection of the personal data by recording reasons in writing within a period of 14 days from the receipt of an application under sub-section (2).

(4) Notwithstanding anything contained in sub-section (2) and sub-section (3), if the Central Government is satisfied that a grave threat to the security of the State or public order exists, it may, for reasons to be recorded in writing, which

shall include the reason for not getting an order under sub-section (3), order the collection of any personal data.

(5) Before the expiry of a period of seven days from the date of an order for collection of personal data made under sub-section (4), the intelligence organisation that collected the personal data shall notify the Chief Privacy Commissioner of the fact of such collection, the name and address of the person to whom the personal data pertains and shall furnish a copy of the order of the Central Government authorising the collection of the personal data.

(6) No intelligence organisation shall process or store any personal data without implementing measures to secure that the number of persons within that intelligence organisation to whom it is made available, and the extent to which it is copied, is limited to the minimum that is necessary to fulfill the purpose for which it is processed or stored, as the case may be.

(7) Any intelligence organisation that processes or stores personal data shall, before the expiry of a period of seven days from the date of the processing or storage, as the case may be, notify the Chief Privacy Commissioner of the fact of such processing or storage and the name and address of the person to whom the personal data pertains.

(8) Any intelligence organisation that processes or stores personal data shall have to comply with the provisions of Section 10 with respect to such data.

CHAPTER IV

Interception of Communications

17. Bar against interception of communications. –

(1) Notwithstanding anything contained in any other law for the time being in force, but save as provided in this chapter, no person shall intercept, or cause to be intercepted, any communication of another person save in pursuance of an order by the Chief Privacy Commissioner or any other person authorised by him in this behalf.

(2) No interception of any communication shall be ordered or carried out that is not necessary to achieve the purpose for which the interception is sought.

18. Prior authorisation by the Chief Privacy Commissioner. –

(1) Any authorised officer seeking to intercept any communication of another person shall prefer an application, in such form and manner as may be prescribed, to the Chief Privacy Commissioner or any other person authorised by him in this behalf.

(2) The Chief Privacy Commissioner, or any other person authorised by him this behalf, may, if he is satisfied that the interception is necessary to prevent a reasonable threat to security of the state or public order, or prevent, investigate or prosecute a cognisable offence, order the interception of communications by

recording reasons in writing within a period of 14 days from the receipt of an application under sub-section (1).

(3) Prior to issuing an order for interception of any communication, the Chief Privacy Commissioner, or any other person authorised by him in this behalf, shall satisfy himself that all other lawful means to acquire the information sought to be intercepted have been exhausted and that the proposed interception is reasonable, proportionate and not excessive.

(4) Any interception of any communication ordered, authorised or carried out prior to the commencement of this Act shall, immediately upon the constitution of the Privacy Commission, be reported to the Chief Privacy Commissioner.

19. Authorisation by Home Secretary in emergent circumstances. –

(1) Notwithstanding anything contained in Section 17, if the Home Secretary of the appropriate government is satisfied that an imminent grave threat to the security of the state or public order exists, he may, for reasons to be recorded in writing, order the interception of any communication.

(2) No order for interception of any communication made under this section shall be valid upon the expiry of a period of seven days from the date of the order.

(3) Before the expiry of a period of seven days from the date of an order for interception made under this section, the person who carried out the interception of communication shall notify the Chief Privacy Commissioner of the fact of such interception, the name and address of the person whose communication is being intercepted, and the duration of the interception and, furthermore, shall furnish a copy of the order of the Home Secretary authorising the interception.

20. Duration of interception. –

(1) An order for interception of any communication shall specify the period of its validity and, upon the expiry of the validity of the order, all interception carried out in relation to that order shall cease forthwith:

Provided that no order for interception of any communication shall be valid upon the expiry of a period of sixty days from the date of the order.

(2) The Chief Privacy Commissioner, or any other person authorised by him in this behalf, may, upon receipt of an application from an authorised officer in such form and manner as may be prescribed, renew any order for interception of any communication if he is satisfied that the conditions upon which the original order was issued continue to exist.

21. Duty to inform the person concerned. –

(1) Subject to sub-section (2), before the expiry of a period of sixty days from the conclusion of any interception of communication ordered or carried out under this Act, the authorised officer who carried out the interception of communication shall, in writing in such form and manner as may be prescribed, notify, with reference to the relevant order of the Chief Privacy Commissioner, each person

whose communication was intercepted of the fact of such interception and duration thereof.

(2) The Chief Privacy Commissioner may, on an application made by an authorised officer in such form and manner as may be prescribed, if he is satisfied that the notification under sub-section (1) would reasonably present a reasonable threat to the security of the state or public order, or adversely affect the prevention, investigation or prosecution of a cognisable offence, for reasons to be recorded in writing addressed to the authorised officer, order that the person whose communication was intercepted not be notified of the fact of such interception or the duration thereof:

Provided any orders passed preventing disclosure of interception under Section (2) shall not operate in infinity and shall record reasons in writing with the period till when the reasonable threat is anticipated to extend, on whose cessation the duty to inform under sub-section (1) will operate.

22. Security and duty of confidentiality and secrecy. –

(1) No person shall intercept any communication of another person without implementing measures, including, but not restricted to, technological, physical and administrative measures, to secure the confidentiality and secrecy of all information obtained as a result of an interception of communication, including from theft, negligence, loss or unauthorised disclosure.

(2) Any person who carries out any interception of any communication, or who obtains any information, including personal data, as a result of an interception of communication, shall be subject to a duty of confidentiality and secrecy in respect of it.

(3) Every competent organisation shall, before the expiry of a period of one hundred days from the enactment of this Act, designate as many officers as it deems fit as Privacy Officers who shall be administratively responsible for all interceptions of communications carried out by that competent organisation.

23. Disclosure of intercepted communications. –

(1) Save as provided in this section, no person shall disclose to any other person, or otherwise cause any other person to come into the knowledge or possession of, the content or nature of any information, including personal data, obtained as a result of an interception of any communication including the fact that the interception of communication was carried out.

(2) Notwithstanding anything contained in this section, if the disclosure of any information, including personal data, obtained as a result of an interception of any communication is necessary to prevent a reasonable threat to the security of the state or public order, or prevent, investigate or prosecute a cognisable offence, an authorised officer may disclose the information, including personal data, obtained as a result of the interception of any communication to any authorised officer of any other competent organisation.

Provided that no authorised officer shall disclose any information, including personal data, obtained as a result of the interception of any communication that is not necessary to achieve the purpose for which the disclosure is sought.

24. Storage of intercepted communications. –

- (1) Subject to sub-section (2), no person shall store any information, including personal data, obtained as a result of an interception of any communication for a period longer than one hundred and eighty days from the date on which the last order for interception of the communication to which the obtained information pertains expired.
- (2) The Chief Privacy Commissioner may, on an application made in such form and manner as may be prescribed, if he is satisfied that it is necessary to prevent a reasonable threat to the security of the state or public order, or to prevent, investigate or prosecute a cognisable offence, for reasons to be recorded in writing, order that any information, including personal data, obtained as a result of an interception of any communication may be stored for a period longer than one hundred and eighty days from the date on which the last order for interception of the communication to which the obtained information pertains expired.
- (3) Any data obtained as a result of interception of any communication shall be stored in a manner that complies with the provisions of Section 9 with respect to such data.

CHAPTER V

Surveillance

25. Bar against surveillance. –

Notwithstanding anything contained in any other law for the time being in force, but save as provided in this chapter, no person shall order or carry out, or cause or assist the ordering or carrying out of, any surveillance of another person.

Provided that there shall be an absolute bar to the subjection of persons to indiscriminate monitoring through any methods of mass or bulk surveillance given that it is neither necessary or proportionate to any stated purpose including but not limited to the security of state, interests of public order or to prevent, investigate or prosecute a commission of a cognisable offence.

26. Surveillance by the State. –

- (1) No member of a police force, armed force, intelligence organisation, public authority or the State shall order or carry out, or cause to be ordered or carried out, any surveillance of another person save in pursuance of an order by the Chief Privacy Commissioner or any other person authorised by him in this behalf.
- (2) No surveillance shall be ordered or carried out that is not necessary to achieve the purpose for which the surveillance is sought.

(3) Any authorised officer seeking to carry out any surveillance of another person shall prefer an application, in such form and manner as may be prescribed, to the Chief Privacy Commissioner or any other person authorised by him in this behalf.

(4) The Chief Privacy Commissioner, or any other person authorised by him this behalf, may, if he is satisfied that the surveillance is necessary to prevent a reasonable threat to the security of the state or public order, or to prevent, investigate or prosecute a cognisable offence, for reasons to be recorded in writing addressed to the authorised officer, order the surveillance.

(5) Prior to issuing an order for surveillance, the Chief Privacy Commissioner, or any other person authorised by him in this behalf, shall satisfy himself that all other lawful means to acquire the information sought to be obtained as a result of the proposed surveillance have been exhausted and that the proposed surveillance is reasonable, proportionate and not excessive.

27. Surveillance by private persons or entities. –

(1) Notwithstanding anything contained in any other law for the time being in force, and without prejudice to the provisions of section 25 of this Act, no person who is not a member of a police force, armed force, intelligence organisation, public authority or the State shall carry out, or cause to be carried out, any surveillance in any public place or in any property or premises that is not in his possession.

(2) Without prejudice to sub-section (1), any person who carries out any surveillance under this section shall be subject to a duty to inform, in such manner as may be prescribed, members of the public of such surveillance.

28. Duration of surveillance. –

(1) An order for surveillance shall specify the period of its validity and, upon the expiry of the validity of the order, all surveillance carried out in relation to that order shall cease forthwith:

Provided that no order for surveillance shall be valid upon the expiry of a period of sixty days from the date of the order.

(2) The Chief Privacy Commissioner, or any other person authorised by him in this behalf, may, upon receipt of an application from an authorised officer in such form and manner as may be prescribed, renew any order for surveillance if he is satisfied that the conditions upon which the original order was issued continue to exist.

29. Duty to inform the person concerned. –

(1) Subject to sub-section (2), before the expiry of a period of sixty days from the conclusion of any surveillance ordered or carried out under this Act, the authorised officer who carried out the surveillance shall, in writing in such form and manner as may be prescribed, notify, with reference to the relevant order of

the Chief Privacy Commissioner, each person in respect of whom surveillance was carried out of the fact of such surveillance and duration thereof.

(2) The Chief Privacy Commissioner may, on an application made by an authorised officer in such form and manner as may be prescribed, if he is satisfied that the notification under sub-section (1) would present a reasonable threat to the security of the state or public order, or adversely affect the prevention, investigation or prosecution of a cognisable offence, for reasons to be recorded in writing addressed to the authorised officer, order that the person not be notified of the fact of such surveillance or the duration thereof:

Provided any orders passed preventing disclosure of surveillance under Section (2) shall not operate in infinity and shall record reasons in writing with the period till when the reasonable threat is anticipated to extend, on whose cessation the duty to inform under sub-section (1) will operate.

30. Security and duty of confidentiality and secrecy. –

(1) No person shall carry out any surveillance of another person without implementing measures, including, but not restricted to, technological, physical and administrative measures, to secure the confidentiality and secrecy of all information obtained as a result of surveillance, including from theft, loss or unauthorised disclosure.

(2) Any person who carries out any surveillance, or who obtains any information, including personal data, as a result of surveillance, shall be subject to a duty of confidentiality and secrecy in respect of it.

(3) Every police force, armed force, intelligence organisation, public authority or State shall, before the expiry of a period of one hundred days from the enactment of this Act, designate as many officers as it deems fit as Privacy Officers who shall be administratively responsible for all surveillance carried out:

Provided that a public authority that does not order or carry out surveillance shall not be required to designate any Privacy Officers under this sub-section.

(4) Every person who is not a member of a police force, armed force, intelligence organisation, public authority or State and who seeks to carry out any surveillance shall, at least seven days before the surveillance is first carried out, designate or appoint as many persons as it deems fit as Privacy Officers who shall be responsible for all surveillance carried out:

Provided that where surveillance is carried out by a single person, that person shall be deemed to be a Privacy Officer.

31. Disclosure of surveillance. –

(1) Save as provided in this section, no person shall disclose to any other person, or otherwise cause any other person to come into the knowledge or possession of, the content or nature of any information, including personal data, obtained as a result of any surveillance including the fact that the surveillance was carried out.

(2) Notwithstanding anything contained in this section, if the disclosure of any information, including personal data, obtained as a result of surveillance is necessary to prevent a reasonable threat to the security of the State or public order, or prevent, investigate or prosecute a cognisable offence, that information, including personal data, obtained as a result of surveillance may be disclosed to a police force, armed force, intelligence organisation, public authority or State only:

Provided that no person shall disclose any information, including personal data, obtained as a result of surveillance that is not necessary to achieve the purpose for which the disclosure is sought.

32. Storage of surveillance. –

(1) Subject to sub-section (2), no person shall store any information, including personal data, obtained as a result of surveillance for a period longer than one hundred and eighty days from the date on which the surveillance to which the obtained information pertains ceased.

(2) The Chief Privacy Commissioner may, on an application made in such form and manner as may be prescribed, if he is satisfied that it is necessary to prevent a reasonable threat to the security of the state or public order, or to prevent, investigate or prosecute a cognisable offence, for reasons to be recorded in writing, order that any information, including personal data, obtained as a result of surveillance may be stored for a period longer than one hundred and eighty days from the date on which the last order for surveillance to which the obtained information pertains expired.

(3) Any data obtained as a result of surveillance shall be stored in a manner that complies with the provisions of Section 9 with respect to such data.

CHAPTER VI

The Privacy Commission

33. Constitution of the Privacy Commission. –

(1) The Central Government shall, by notification, constitute, with effect from such date as may be specified therein, a body to be called the Privacy Commission consisting of a Chief Privacy Commissioner and not more than six other Privacy Commissioners, to be appointed by the President, by warrant under its hand and seal, to exercise the jurisdiction and powers and discharge the functions and duties conferred or imposed upon them by or under this Act.

(2) The Chief Privacy Commissioner shall be a person who has been a Judge of the Supreme Court of India:

(3) One Privacy Commissioner shall be a person who is or has been a Judge of a High Court:

(4) One Privacy Commissioner shall be a person of ability, integrity and standing who has a special knowledge of, and professional experience of not less than ten

years in privacy law and policy.

(5) The other Privacy Commissioners shall be persons with technical expertise and knowledge in the fields of data collection and storage practices, or data protection and ethics, or big data analytics and technologies or information technology while one Privacy Commissioner should be an ordinary citizen representing the interests of the public who are consumers of data.

(6) The office of the Privacy Commission shall be autonomous, independent, and free from external interference. The Office shall be provided with sufficient operational resources including human, technical, and financial for the effective discharge of its duties and exercise of its powers. Such powers shall be subject to audit by the Comptroller and Auditor General of India.

(8) The Central Government shall issue a public advertisement inviting applications to fill all vacancies in the Privacy Commission. The selection committee for the appointment of the members of the Privacy Commission shall comprise the Chief Justice of India, the Law Minister, the Leader of the Opposition from Lok Sabha or of the single largest Opposition party being one with the greatest numerical strength in the Lok Sabha, one eminent person representing the private sector and one eminent person representing the civil society. All proceedings of the selection committee will constitute a public record.

Explanation: “Civil society” shall mean the aggregate of non-governmental and non-profit organisations that perform activities for the general upliftment and interests of the people in the field of privacy and is independent of government funding, interference or influence.

34. Term of office, conditions of service, etc. of Chief Privacy Commissioner and Privacy Commissioners. –

(1) Before appointing any person as the Chief Privacy Commissioner or Privacy Commissioner, the President shall satisfy himself or herself that the person does not, and will not, have any such financial or other interest as is likely to affect prejudicially their functions as such Chief Privacy Commissioner or Privacy Commissioner.

(2) The Chief Privacy Commissioner and every Privacy Commissioner shall hold office for such period, not exceeding five years, as may be specified by the President in the order of his appointment, but shall be eligible for reappointment:

Provided that no person shall hold office as the Chief Privacy Commissioner or Privacy Commissioner for more than two terms.

Provided that no person shall hold office as the Chief Privacy Commissioner or Privacy Commissioner after they have attained the age of 75 years.

(3) Notwithstanding anything contained in sub-section (2), the Chief Privacy Commissioner or any Privacy Commissioner may –

(a) by writing under his hand and addressed to the President resign his office at any time;

(b) be removed from office in accordance with the provisions of Section 35 of this Act.

(4) A vacancy caused by the resignation or removal of the Chief Privacy Commissioner or Privacy Commissioner under sub-section (3) shall be filled by fresh appointment.

(5) In the event of the occurrence of a vacancy in the office of the Chief Privacy Commissioner, such one of the Privacy Commissioners as the President may, by notification, authorise in this behalf, shall act as the Chief Privacy Commissioner till the date on which a new Chief Privacy Commissioner, appointed in accordance with the provisions of this Act, to fill such vacancy, enters upon his office.

(6) When the Chief Privacy Commissioner is unable to discharge his functions owing to absence, illness or any other cause, such one of the Privacy Commissioners as the Chief Privacy Commissioner may authorise in writing in this behalf shall discharge the functions of the Chief Privacy Commissioner, till the date on which the Chief Privacy Commissioner resumes his duties.

(7) The salaries and allowances payable to and the other terms and conditions of service of the Chief Privacy Commissioner and Privacy Commissioners shall be such as may be prescribed:

Provided that neither the salary and allowances nor the other terms and conditions of service of the Chief Privacy Commissioner and any Privacy Commissioner shall be varied to their disadvantage after their appointment.

(8) The Chief Privacy Commissioner and Privacy Commissioners ceasing to hold office as such shall not hold any appointment under the Government of India or under the Government of any State for a period of five years from the date on which they cease to hold such office.

35. Removal of Chief Privacy Commissioner and Privacy Commissioners from office in certain circumstances. –

(1) The President may remove from office the Chief Privacy Commissioner or any Privacy Commissioner, who –

(a) is adjudged an insolvent; or

(b) engages during his term of office in any paid employment outside the duties of his office; or

(c) is unfit to continue in office by reason of infirmity of mind or body; or

(d) is of unsound mind and stands so declared by a competent court; or

(e) is convicted for an offence which in the opinion of the President involves moral turpitude; or

(f) has acquired such financial or other interest as is likely to affect prejudicially his functions as a Chief Privacy Commissioner or Privacy Commissioner, or cause some conflict of interest including benefits directly or indirectly to relatives or family members, or

(g) has so abused his position as to render his continuance in offence prejudicial to the public interest.

(2) Notwithstanding anything contained in sub-section (1), neither the Chief Privacy Commissioner nor any Privacy Commissioner shall be removed from his office on the ground specified in clause (f) or clause (g) of that sub-section unless the Supreme Court on a reference being made to it in this behalf by the President, has on an inquiry held by it in accordance with such procedure as it may specify in this behalf, reported that the Chief Privacy Commissioner or Privacy Commissioner ought, on such grounds, to be removed.

36. Functions of the Privacy Commission. –

(1) The Privacy Commission may, through decisions arrived at by a simple majority of its members present and voting as set out in Section 44(1) of this Act, authorise, review, investigate, make an inquiry, and/or monitor, *suo moto* or on a petition presented to it by any person or by someone acting on his behalf, the implementation and application of this Act and give such directions or pass such orders as are necessary for reasons to be recorded in writing.

(2) Without prejudice to the generality of the foregoing provision, the Privacy Commission shall perform all or any of the following functions, namely –

1. a) review the safeguards provided under this Act and under other laws for the time being in force for the protection of personal data and recommend measures for their effective implementation or amendment, as may be necessary from time to time;

(b) authorise, review, investigate, make an inquiry, and/or monitor any measures taken by any competent organisation, police force, armed force, intelligence organisation, public authority, company, person or other entity for the protection of privacy and take such further action as it deems fit;

(c) authorise, review, investigate, make an inquiry, and/or monitor any action, code, certification, policy or procedure of any competent organisation, police force, armed force, intelligence organisation, public authority, company, person or other entity to ensure compliance with this Act and any rules made hereunder;

(d) Investigate and direct data controllers and processors to do or cease to do any act in order to address activity which is in contravention of the provisions of this Act

(e) formulate through public consultation with experts, other stakeholders, and the general public, norms for the effective protection of privacy by competent organisations, police forces, armed forces, intelligence organisations, public authorities, companies, persons or other entities;

- (f) promote awareness and knowledge of personal data protection through any means necessary and to all stakeholders including providing information to any data subject regarding their rights under this Act as requested ;
 - (g) undertake and promote research in the field of protection of personal data and privacy;
 - (h) encourage the efforts of non-governmental organisations and institutions working in the field of personal data protection and privacy;
 - (i) publish periodic reports concerning the incidence of compliance including violations of this Act and data breaches as reported under Chapter III section 11(4) of this Act, collection, processing, storage, disclosure and other handling of personal data, interception of communications and surveillance;
 - (j) hear and decide applications for interception and surveillance under Chapters IV and V of this Act;
 - (k) exercise its powers under Section 28, to ensure the speedy and efficient redressal of all complaints whose cause of action arises from this Act;
 - (l) such other functions as it may consider necessary for the protection of privacy, personal data, and enforcement of this Act.
- (3) The Periodic Reports published by the Privacy Commission, stipulated in Section 36(2)(i), shall be tabled before the Lok Sabha by the Law Minister during the Parliamentary Session that succeeds the publication of any Periodic Report.
- (4) The Chief Privacy Commissioner and the Privacy Commissioners shall appear before a special *ad hoc* Committee, constituted by the Speaker of the Lok Sabha and comprising of members from both the governing and the opposition parties from both houses of Parliament, on an annual basis, in a manner that may be prescribed by rules.
- (i) The *ad hoc* Committee shall be empowered to review the functioning of the Privacy Commission, and may ask the Chief Privacy Commissioner and the Privacy Commissioners any questions in this regard, as per rules.
 - (ii) The *ad hoc* Committee will function and present periodic reports to both houses of Parliament in a manner prescribed as per the rules.
- (5) Subject to the provisions of any rules prescribed in this behalf by the Central Government, the Privacy Commission shall have the power to review any decision, judgement, decree or order made by it.
- (6) In the exercise of its functions under this Act, the Privacy Commission shall give such directions or pass such orders as are necessary for reasons to be recorded in writing.
- (7) The Privacy Commission may, in its own name, sue or be sued.

37. Secretary, officers and other employees of the Privacy Commission. –

- (1) The Central Government shall appoint a Secretary to the Privacy Commission to exercise and perform, under the control of the Chief Privacy Commissioner such powers and duties as may be prescribed or as may be specified by the Chief Privacy Commissioner.
- (2) The Central Government may provide the Privacy Commission with such other officers and employees as may be necessary for the efficient performance of the functions of the Privacy Commission.
- (3) The salaries and allowances payable to and the conditions of service of the Secretary and other officers and employees of the Privacy Commission shall be such as may be prescribed.

38. Salaries, etc. be defrayed out of the Consolidated Fund of India.

—

The salaries and allowances payable to the Chief Privacy Commissioner and Privacy Commissioners and the administrative expenses, including salaries, allowances and pension, payable to or in respect of the officers and other employees of the Privacy Commission shall be defrayed out of the Consolidated Fund of India.

39. Vacancies, etc. not to invalidate proceedings of the Privacy Commission. –

No act or proceeding of the Privacy Commission shall be questioned on the ground merely of the existence of any vacancy or defect in the constitution of the Privacy Commission or any defect in the appointment of a person acting as the Chief Privacy Commissioner or Privacy Commissioner.

40. Chief Privacy Commissioner, Privacy Commissioners and employees of the Privacy Commission to be public servants. –

The Chief Privacy Commissioner and Privacy Commissioners and other employees of the Privacy Commission shall be deemed to be public servants within the meaning of section 21 of the Indian Penal Code, 1860 (45 of 1860).

41. Location of the office of the Privacy Commission. –

The offices of the Privacy Commission shall be in New Delhi or any other location as directed by the Chief Privacy Commissioner in consultation with the Central Government.

42. Procedure to be followed by the Privacy Commission. –

- (1) Subject to the provisions of this Act, the Privacy Commission shall have powers to regulate —
 - (a) the procedure and conduct of its business;

(b) the delegation to one or more Privacy Commissioners of such powers or functions as the Chief Privacy Commissioner may specify.

(2) In particular and without prejudice to the generality of the foregoing provisions, the powers of the Privacy Commission shall include the power to determine the extent to which persons interested or claiming to be interested in the subject-matter of any proceeding before it may be allowed to be present or to be heard, either by themselves or by their representatives or to cross-examine witnesses or otherwise take part in the proceedings:

Provided that any such procedure as may be prescribed or followed shall be guided by the principles of natural justice.

43. Power relating to inquiries. –

(1) The Privacy Commission shall, for the purposes of any inquiry or for any other purpose under this Act, have the same powers as vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying suits in respect of the following matters, namely –

- (a) the summoning and enforcing the attendance of any person from any part of India and examining him on oath;
- (b) the discovery and production of any document or other material object producible as evidence;
- (c) the reception of evidence on affidavit;
- (d) the requisitioning of any public record from any court or office;
- (e) the issuing of any commission for the examination of witnesses; and,
- (f) any other matter which may be prescribed.

(2) The Privacy Commission shall have power to require any person, subject to any privilege which may be claimed by that person under any law for the time being in force, to furnish information on such points or matters as, in the opinion of the Privacy Commission, may be useful for, or relevant to, the subject matter of an inquiry and any person so required shall be deemed to be legally bound to furnish such information within the meaning of section 176 and section 177 of the Indian Penal Code, 1860 (45 of 1860).

(3) The Privacy Commission or any other officer, not below the rank of a Gazetted Officer, specially authorised in this behalf by the Privacy Commission may enter any building or place where the Privacy Commission has reason to believe that any document relating to the subject matter of the inquiry may be found, and may seize any such document or take extracts or copies therefrom subject to the provisions of section 100 of the Code of Criminal Procedure, 1973 (2 of 1974), in so far as it may be applicable.

(4) The Privacy Commission shall be deemed to be a civil court and when any offence as is described in section 175, section 178, section 179, section 180 or

section 228 of the Indian Penal Code, 1860 (45 of 1860) is committed in the view or presence of the Privacy Commission, the Privacy Commission may, after recording the facts constituting the offence and the statement of the accused as provided for in the Code of Criminal Procedure, 1973 (2 of 1974), forward the case to a Magistrate having jurisdiction to try the same and the Magistrate to whom any such case is forwarded shall proceed to hear the complaint against the accused as if the case had been forwarded to him under section 346 of the Code of Criminal Procedure, 1973 (2 of 1974).

44. Decisions of the Privacy Commission. –

(1) The decisions of the Privacy Commission shall be taken by majority and be binding and enforceable as a decree of a court as per the provisions of the Code of Civil Procedure, 1908.

(2) In its decisions, the Privacy Commission has the power to –

(a) require a competent organisation, police force, armed force, intelligence organisation, public authority, company, person or other entity to take such steps as may be necessary to secure compliance with the provisions of this Act;

(b) require a competent organisation, police force, armed force, intelligence organisation, public authority, company, person or other entity to compensate any person for any loss or detriment suffered;

(c) impose any of the penalties provided under this Act.

45. Proceedings before the Privacy Commission to be judicial proceedings. –

The Privacy Commission shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973 (2 of 1974), and every proceeding before the Privacy Commission shall be deemed to be a judicial proceeding within the meaning of section 193 and section 228 and for the purposes of section 196 of the Indian Penal Code, 1860 (45 of 1860).

CHAPTER VI-A

Regulation by Data Controllers and Data Processors

46. Co-regulation by Data Controllers and the Privacy Commission.

—

(1) Without prejudice to the provisions of clause (d) of sub-section (2) of section 36, the Privacy Commission may, after a public consultation, formulate codes of conduct for the collection, storage, processing, disclosure or other handling of any personal data.

(2) No code of conduct formulated under sub-section (1) shall be binding on a data controller unless –

(a) it has received the written approval of the Chief Privacy Commissioner and at least two Privacy Commissioners; and

(b) it has received the approval, by signature of a director or authorised signatory, of the data controller.

47. Self-regulation by data controllers. –

(1) The Privacy Commission may encourage data controllers and data processors to formulate professional codes of conduct to establish rules for the collection, storage, processing, disclosure or other handling of any personal data.

(2) No code of conduct formulated under sub-section (1) shall be effective unless it is registered, in such form and manner as may be prescribed, by the Privacy Commission.

(3) The Privacy Commission shall, for reasons to be recorded in writing, not register any code of conduct formulated under sub-section (1) that is not adequate to protect personal data.

48. Co-regulation & Self-regulation without prejudice to other remedies. –

Any code of conduct formulated under this chapter shall be without prejudice to the jurisdiction, powers and functions of the Privacy Commission.

CHAPTER VII

Offences and penalties

49. Punishment for offences related to personal data. –

(1) Whoever, except in conformity with the provisions of this Act, collects, receives, stores, processes, discloses or otherwise handles any personal data shall be liable to fine which may extend to 1 crore rupees.

Provided that whoever commits the offence defined above either intentionally, or with reckless disregard, shall be liable for a term of imprisonment extending upto three years, and shall also be liable to fine.

(2) Whoever attempts to commit any offence under sub section (1) shall be liable in the manner and to the extent provided for such offence under that sub-section.

(3) Whoever, except in conformity with the provisions of this Act, collects, receives, stores, processes, discloses or otherwise handles any sensitive personal data shall be liable to fine which may extend to 10 crore rupees.

Provided that whoever commits the offence defined above either intentionally, or with reckless disregard, shall be liable for a term of imprisonment extending upto five years, and shall also be liable to fine.

(4) Whoever attempts to commit any offence under sub section (3) shall be punishable with the punishment provided for such offence under that sub-section.

50. Punishment for offences related to interception of communication. –

(1) Whoever, except in conformity with the provisions of this Act, intercepts, or causes the interception of, any communication of another person shall be liable to a fine which may extend to 1 crore rupees.

Provided that whoever commits the offence defined above either intentionally, or with reckless disregard, shall be liable for a term of imprisonment extending upto three years, and shall also be liable to fine.

(2) Whoever attempts to commit any offence under sub section (1) shall be punishable with the punishment provided for such offence under that sub section.

51. Punishment for offences related to surveillance. –

(1) Whoever, except in conformity with the provisions of this Act, orders or carries out, or causes the ordering or carrying out, of any surveillance of another person shall be liable to a fine which may extend to 10 crore rupees.

Provided that whoever commits the offence defined above either intentionally, or with reckless disregard, shall be liable for a term of imprisonment extending upto five years, and shall also be liable to fine.

(2) Whoever attempts to commit any offence under sub section (1) shall be punishable with the punishment provided for such offence under that sub section.

52. Abetment and repeat offenders. –

Whoever abets any offence punishable under this Act shall, if the act abetted is committed in consequence of the abetment, be punishable with the punishment provided for that offence.

53. Offences by companies. –

(1) Where an offence under this Act has been committed by a company, every person who, at the time of the offence was committed, was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to any punishment, if he proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence.

(2) Notwithstanding anything contained in sub-section (1), where any offence under this Act has been committed by a company and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any neglect on the part of any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall be deemed to be guilty of that offence, and shall be liable to be proceeded against and punished accordingly.

54. Cognisance. –

Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), the offences under this chapter shall be cognisable and non-bailable.

55. General penalty. –

Whoever, in any case in which a penalty is not expressly provided by this Act, fails to comply with any notice or order issued under any provisions thereof, including an order of the Chief Privacy Commissioner or otherwise contravenes any of the provisions of this Act, shall be punishable with fine which may extend to 1 crore rupees, and, in the case of a continuing failure or contravention, with an additional fine which may extend to 10 lakh rupees for every day after the first during which he has persisted in such failure or contravention.

56. Punishment to be without prejudice to any other action. –

The award of punishment for an offence under this Act shall be without prejudice to any other action which has been or which may be taken under this Act with respect to such contravention.

CHAPTER VIII

Miscellaneous

57. Power to make rules. –

- (1) The Central Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.
- (2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for –
 - (a) the notification of theft, loss or damage under sub-section (4) of section 11;
 - (c) the notification of disclosure under sub-section (4) of section 13;
 - (d) the application by an intelligence organisation under sub-section (2) of section 15;
 - (e) the application to intercept a communication under sub-section (1) of section 18;
 - (f) the application to renew an interception of communication under sub-section (2) of section 20;
 - (g) the notification of an interception of communication under sub-section (1) of section 21;
 - (h) the application to not inform under sub-section (2) of section 21;
 - (i) the application to store information obtained as a result of any interception of communication under sub-section (2) of section 24;
 - (j) the application to carry out surveillance under sub-section (3) of section 26;
 - (k) notification to the general public under sub-section (2) of section 27;

- (m) the application to renew surveillance under sub-section (2) of section 28;
- (n) the notification of surveillance under sub-section (1) of section 29;
- (o) the application to not inform under sub-section (2) of section 29;
- (p) the application to store information obtained as a result of surveillance under sub-section (2) of section 32;
- (q) salaries, allowances and other terms and conditions of service of the Chief Privacy Commissioner, Privacy Commissioners, Secretaries and other members, staff and employees of the Privacy Commission;
- (r) procedure to be followed by the Privacy Commission;
- (s) powers and duties of Secretaries, officers and other employees of the Privacy Commission;
- (t) the effective implementation of this Act.

(3) Every rule made under this section shall be laid, as soon as may be after it is made, before each House of Parliament while it is in session for a period of thirty days which may be comprised in one session or in two successive sessions and if before the expiry of the session in which it is so laid or the session immediately following, both Houses agree in making any modification in the rule, or both Houses agree that the rule should not be made, the rule shall thereafter have effect only in such modified form or be of no effect, as the case may be, so however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule.

58. Bar of jurisdiction. –

(1) On and from the appointed day, no court or authority shall have, or be entitled to exercise, any jurisdiction, powers or authority (except the Supreme Court and a High Court exercising powers under Article 32, Article 226 and Article 227 of the Constitution) in relation to matters over which the Privacy Commission has jurisdiction.

(2) No order passed under this Act shall be appealable except as provided therein and no civil court shall have jurisdiction in respect of any matter which the Privacy Commission is empowered by, or under, this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

59. Protection of action taken in good faith. –

No suit or other legal proceeding shall lie against the Central Government, State Government, Privacy Commission, Chief Privacy Commissioner, Privacy Commissioner or any person acting under the direction either of the Central Government, State Government, Privacy Commission, Chief Privacy Commissioner or Privacy Commissioner in respect of anything which is in good faith

done or intended to be done in pursuance of this Act or of any rules or any order made thereunder.

60. Power to remove difficulties. –

(1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order, published in the Official Gazette, make such provisions, not inconsistent with the provisions of this Act, as appears to it to be necessary or expedient for removing the difficulty:

Provided that no such order shall be made under this section after the expiry of a period of three years from the commencement of this Act.

(2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

61. Act to have overriding effect. – Subject to the provisions of Schedule A, the provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

SCHEDULE A

1. Statutes, provisions whereof, shall have to comply with the requirements of this Act
2000. a) Sections 43A, 69, 69B, 72 and 72A of the Information Technology Act, 2000.
2016. c) Sections 28, 29, 30, 31, 32 and 33 of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016.
2017. d) Section 5(2) of the Indian Telegraph Act, 1885
 1. f) Section 21 of the Prevention of Money Laundering Act, 2002
 2. g) The Census Act, 1948
1. Statutes, provisions whereof shall not be required to comply with the provisions of this Act
 1. The Representation of the People Act, 1951
 2. The Right to Information Act, 2005

FINANCIAL MEMORANDUM

1. Clause 33(1) provides for establishment of the Privacy Commission which shall be a body corporate having perpetual succession and a common seal with power to acquire, hold and dispose of property and sue or be sued with an office as determined under Clause 41.
2. Clause 33(1) provides that the Privacy Commission shall consist of a Chief Privacy Commissioner and six other members as Privacy Commissioners.

3. Sub-clause 7 of clause 34 makes provision for salaries and allowances payable to the Chief Privacy Commissioner and allowances or remuneration payable to the Privacy Commissioners.
4. Clause 37 provides for the appointment of a secretary, officers and other employees of the Privacy Commission,
5. Clause 38 provides that the expenditure for the Privacy Commission shall be incurred from the Consolidated Fund of India. The Bill, therefore, if enacted, would involve expenditure from the Consolidated Fund of India. The Bill, if enacted, would involve a recurring expenditure of about rupees six hundred crore per annum. A non-recurring expenditure of about rupees one hundred and twenty five crore is also likely to be involved.

STATEMENT OF OBJECTS AND REASONS

Our country is at the threshold of a new technological revolution, marrying welfare with programmes of digitization for the quick and effective delivery of government services and benefits from various schemes. For this process, ranging from electronic banking to the transfer of subsidies, vast amounts of data are collected from our citizens, the integrity of which must be protected. This data can be used for seemingly innocuous purposes such as targeted advertising but also for provision of essential services such as ration, credit, insurance, and more, while unprotected and in the wrong hands, it could also cause damage to the interests of the individual.

Beyond its commercial exploitation there is also an inherent equation of power when a person or entity possesses data and information concerning another individual or groups of individuals. Today, most such interactions are unregulated and put the users of internet and technological services at risk, and this risk will only grow with more and more digitization and as technological involvement in the delivery of services to citizens develops.

Many concerns arise from the absence of a comprehensive data protection and privacy statute which provides rights to individuals in a data governed world. This has been recognized by past efforts of the Government of India notably by the Report of the Group of Experts on Privacy chaired by Justice A.P. Shah, Former Chief Justice, Delhi High Court. Drawing on the recommendations of this expert group, global best practices and also the unique factors that exist locally, this Data Privacy And Protection Bill aims to provide a comprehensive law to protect privacy and data collected from our citizens.

This bill puts a person in control of his/her own data and further permits them to make an informed choice concerning its use. The Bill further provides an industry friendly model of co-regulation that aims to foster a higher degree of certainty for the private sector. The concerns of government are also sought to be addressed with a balanced provision for interception and access, making special provisions to safeguard the security of the state. The aims and objectives of the bill are sought to be implemented by an autonomous privacy commission.

The Data Privacy and Protection Bill, 2017 aims to protect and promote our constitutional ideals in a networked, increasingly digitized society.

Therefore, this Bill.

SHASHI THAROOR

New Delhi; July 2, 2017

NOTES ON CLAUSES

CHAPTER I

Preliminary

Clause 1 contains the title of the proposed legislation – the Data Privacy And Protection Act, 2017. This legislation takes individuals' rights to the protect and control their identities and information concerning them to be necessary entailments of the right to life and personal liberty guaranteed in Article 21 of the Constitution. Recognizing the various circumstances in which offshore transfers of data pertaining to Indian residents may occur and with a view to enabling the preservation and defence of their right to privacy, this clause also enables the provisions of this legislation to have effect outside India.

Clause 2 seeks to define words and expressions used in the proposed legislation. It specifically defines the types of data, and the various uses it can be put to.

Clause 3 enumerates various principles that ought to guide the working of this legislation. This legislation recognizes the utility of data to governments and commercial actors alike, and is intended to ensure that data subjects are treated as owners of information pertaining to them. It also acknowledges both that privacy is indispensable to democratic life, and that international law, including human rights treaties, oblige India to preserve democracy by limiting intrusions into privacy to those which are necessary and proportional. In order to secure this aim, this legislation envisages the establishment of a competent, well-funded and independent regulator, called the Privacy Commission.

CHAPTER II

Right to Privacy

Clause 4 codifies the right to privacy necessarily implicit in Article 21 of the Constitution into statute, and mandates that all handling of data, interception and other types surveillance be undertaken strictly in terms of this legislation. A failure to comply with these requirements will be visited with civil and criminal consequences as detailed in Chapter VI.

Clause 5 excepts data handling for two purposes from the rule in clause 4 that all data must be handled in terms of this legislation alone: (1) personal or family use of one's own data and (2) surveillance of one's own residence. These exceptions are intended to preserve the autonomy and enhance the privacy of data subjects in their homes and family lives.

CHAPTER III

Protection of Personal Data

Clause 6 seeks to enumerate conditions precedent to rendering consent, as defined in cl. 2(j), effective for the purposes of this legislation. Similar concerns as those raised by the yawning disproportionalities in bargaining power of the consumer and the service provider that arise in standard form contracts such as those for insurance arise in nearly all contracts which enable the collection of data. Given that consent in the digital age has been reduced to mere formality by the advent of clickwrap contracts, this position seeks to rehabilitate the data subject as a party who has genuine and meaningful autonomy concerning the contexts and ways in which data about her are collected, stored, used and disseminated.

Sub-clause 1 imports the meaning given to ‘free consent’ in the Indian Contract Act, 1872, which contains the various grounds on which consent could be vitiated, into this legislation.

Sub-clause 2 sets up a default rule as to prior consent. Exceptions to this rule are codified in cl.8.

Sub-clause 3 attempts to ensure that consent obtained data subjects is verifiably voluntary. It does so by making it necessary for consent to be indicated affirmatively and for it to be reduced to writing, and by disallowing practices that disallow easy withdrawal of that consent.

Sub-clause 4 requires contracts to be drafted in language that a lay individual can easily comprehend. Given that these will be standard form contracts, it attempts to enforce this requirement by making the contra proferentem rule, by which contracts are read against the interest of the draftsman (who will be the data controller or processor, typically) in case of ambiguity, expressly applicable them.

Sub-clause 5 codifies the principle of purpose limitation, by requiring that consent be sought for clearly demarcated purposes, and thus excluding omnibus or infinite consent from the purview of effective consent.

Clause 7 explains the requirements for lawful data collection and use under this legislation. It implements the effective consent requirement, expressly limits permissible collection to cases where it is necessary to achieve a stated purpose, lists the elements of a complete notice required to ensure that the data subject is informed in accordance with cl. 6 (4), and requires data destruction on the withdrawal of consent.

Clause 8 contains a list of three exceptions to the rule under cl. 6 (2), by which all consent must be obtained prior to collection and handling of data.

Clause 9 seeks to undo the prevalent practice of data retention for unspecified lengths of time, even after the purpose for which the data was initially collected has lapses. It does so by limiting the duration for which data may be retained

to the life of the purpose for its collection, and instituting a data destruction requirement after that period is completed. Subject to the requirements of proportionality and anonymisation, there are three exceptions to this rule: (1) where effective consent is obtained for the retention, (2) where it is required as evidence in court, and (3) where a statute requires continued retention for one of the reasons specified in sub-clause (3). By operation of clauses 24 and 32, these provisions are made applicable to data collected in the course of interception and surveillance as well.

Clause 10 concerns the standards to be observed when processing personal data. Data processing, like collection, is to be limited to its specified purpose, and altered purposes require fresh effective consent to be obtained. The rule as to purpose limitation may not apply in case of the four exceptions contained in sub-clause 4, which include the maintenance of public safety and the preservation of law and order.

Clause 11 enumerates the obligations that attend the collection and use of personal data. All possible measures to ensure the integrity and secrecy of databases are required to be taken, all persons who come on contact with data are placed under a duty of secrecy and confidentiality in respect of it, and are obligated to report breaches of the standards set down in this Chapter to the statutory regulator upon becoming aware of any such breach.

Clause 12 requires that any transfers of data from controllers to processors be under an agreement that meets, as a minimum standard, all the requirements of this legislation, and continues to hold the person making such a transfer liable to the data subject.

Clause 13 concerns the conditions to be satisfied for lawful disclosures of personal data. It provides that data may only be disclosed with the effective consent of the data subject, and specifies the contents of the notice that must be communicated to the data subject prior to obtaining this consent and restates the requirement in cl. 12 that disclosures by which data is transferred must be by agreement that meets the standards enumerated in this legislation.

Clause 14 requires that all records of personal data be kept accurate, and confers on data subjects the affirmative right to call for records pertaining to them and demand corrections in cases of inaccuracy and destruction where the purpose of the collection or use has lapsed.

Clause 15 makes special provisions in respect of sensitive personal data, requiring that collection and processing be with effective consent and limited to its purpose, that retention be for no longer than is strictly necessary and that no disclosures of or about records of sensitive data be made in any circumstances.

Clause 16 makes special provisions in respect of intelligence organisations. Intelligence agencies under the state operate with great opacity in India, and this provision attempts to subject them to the oversight of the Privacy Commission and to the rigours of this legislation to the extent that they are involved in the

secret – and thus far, unregulated – collection, processing and disclosure of vast amounts of sensitive and ordinary personal data.

CHAPTER IV

Interception of Communications

Clause 17 provides that interception must be undertaken only where necessary and with prior authorization, unless emergent circumstances in terms of cl. 19 arise. Its provisions are intended to supercede the other applicable provisions in statute and delegated legislation including those contained in the Indian Telegraph Act, 1885 and the Information Technology Act, 2000.

Clause 18 lays down standards for procedural and substantive legality of interception. It intends to strike a fair balance between interception targets' right to privacy in their communications and the state's interest in public safety and law and order on the other by providing for narrow and closely overseen channels for interception. Substantively, it requires that all interception be undertaken as a last resort to achieve a clearly specified and lawful purpose, through means which are limited and proportionate to that purpose. Procedurally, it requires that all interception be warranted by a written and reasoned order of an authority separate and independent from those seeking to intercept, and be undertaken only by officers of the government who are specifically authorised to do so.

Clause 19 permits the Home Secretary to warrant interception by a reasoned order in the exceptional cases where there is an imminent and grave threat to security of the state or to public order. Such an order may operate for no longer than 7 days, and its particulars, along with a copy of its contents must be furnished to the Chief Privacy Officer within that time. This provision is intended to be used as sparingly as possible.

Clause 20 attempts to limit privacy invasions caused by surveillance and foster proportionality, by placing a cap on the length of any given instance of surveillance to 60 days, and requiring a review upon application of the reasons for continuing surveillance.

Clause 21 requires, as a general rule, that targets of interception be notified of the fact of such surveillance and of the lengths of time for which they were surveilled. This provision recognizes the dangers to fundamental rights, including privacy and those contained in Article 19 of the Constitution, and to democratic order posed by secret interception. Being that knowledge of a violation of one's rights is a necessary prerequisite to pursuing a redressal, this provision attempts to create a clear avenue for targets of interception to access judicial remedies where necessary.

Clause 22 places all those involved with interception under a duty of confidentiality and secrecy, and requires that all possible measures be taken in advance to ensure that fruits of interception remain secret.

Clause 23 bars the disclosure of the fact, duration and fruits of all interception,

except in cases where such a disclosure is necessary to prevent, investigate or prosecute cognizable offences, including those that threaten the security of the state or public order.

Clause 24 contains a mandatory data destruction requirement and a standard for the storage of the fruits of interception. Per the data destruction requirement, fruits of interception may not be held 180 days after the interception has ended, unless a written and reasoned order to the contrary is obtained. The standard for storage of any data resulting from interception is the same as is provided for in ordinary cases under cl. 9.

CHAPTER V

Surveillance

Clause 25 provides that all surveillance must comply with the provisions of Chapter V of this legislation. Further, it bans the rampant, unregulated practice of dragnet surveillance as being irrevocably incompatible with standards of necessity, proportionality that any invasion into fundamental rights must satisfy both at international human rights law and under the Indian Constitution.

Clause 26 lays down standards for procedural and substantive legality of state surveillance. It intends to strike a fair balance between surveillance targets' right to privacy in their communications and the state's interest in public safety and law and order on the other by providing for narrow and closely overseen channels for surveillance. Substantively, it requires that all state surveillance be undertaken as a last resort to achieve a clearly specified and lawful purpose, through means which are limited and proportionate to that purpose. Procedurally, it requires that all state surveillance be warranted by a written and reasoned order of an authority separate and independent from those seeking to surveil, and be undertaken only by officers of the government who are specifically authorised to do so.

Clause 27 sets up the default rule that surveillance may not be undertaken by private entities, even in public places in the recognition that privacy inheres in persons rather than in places or objects alone.

Clause 28 attempts to limit privacy invasions caused by surveillance and foster proportionality, by placing a cap on the length of any given instance of surveillance to 60 days, and requiring a review upon application of the reasons for continuing surveillance.

Clause 29 requires, as a general rule, that targets of surveillance be notified of the fact of such surveillance and of the lengths of time for which they were surveilled. This provision recognizes the dangers to fundamental rights, including privacy and those contained in Article 19 of the Constitution, and to democratic order posed by secret surveillance. Being that knowledge of a violation of one's rights is a necessary prerequisite to pursuing a redressal, this provision attempts to create a clear avenue for targets of surveillance to access judicial remedies where necessary.

However, this clause also recognizes that investigations into grave threats to national security and the like may justify denying targets, such as those verifiably involved in continuing terrorist activity at a national scale, of their right to notification of surveillance. This denial must always be for reasons and a time period recorded in advance, so that on the expiry of the relevant, the target's right to be notified revives.

Clause 30 places all those involved with surveillance under a duty of confidentiality and secrecy, and requires that all possible measures be taken in advance to ensure that fruits of surveillance remain secret.

Clause 31 bars the disclosure of the fact, duration and fruits of all surveillance, except in cases where such a disclosure is necessary to prevent, investigate or prosecute cognizable offences, including those that threaten the security of the state or public order.

Clause 32 contains a mandatory data destruction requirement and a standard for the storage of the fruits of surveillance. Per the data destruction requirement, fruits of surveillance may not be held 180 days after the surveillance has ended, unless a written and reasoned order to the contrary is obtained. The standard for storage of any data resulting from surveillance is the same as is provided for in ordinary cases under cl. 9.

CHAPTER VI

The Privacy Commission

Clause 33 sets up a Privacy Commission, the statutory regulator under this legislation, set up under the Central government but intended to operate autonomously. It attempts to set up a regulator with a fairly balanced composition headed by a retired Judge of the Supreme Court. Members of the Commission would be drawn from persons having legal or technical expertise with privacy and data protection matters, through a transparent selection process which would include civil society representation.

Clause 34 sets out the terms of office, conditions of service and emoluments due to members of the Privacy Commission. *Inter alia*, it precludes the appointment of any person having financial interests in data protection, caps the number of terms to two terms of 5 years each and provides for a cooling off period of 5 years before members can undertake other appointments under the Central Government.

Clause 35 specifies the grounds for removal of members of the Privacy Commission and specifies the cases in which such removal must be preceded by an inquiry.

Clause 36 details the functions of the Privacy Commission, provides that it will operate by simple majority, pass written and reasoned orders and allows it the power of review over its own decisions. It also renders the Commission accountable to Parliament, and treats the Commission as a legal person capable of suing and being sued.

Clause 37 concerns staffing of the Privacy Commission. It requires that a Secretary be appointed by the Central Government under the Chief Privacy Commissioner. It also allows for the Central Government to appoint other employees, as necessary.

Clause 38 provides that members and employees of the Privacy Commission will be paid from the Consolidated Fund of India.

Clause 39 provides that defects in the constitution of the Privacy Commission or of appointment of its members do not themselves constitute a ground for impugning proceedings conducted by the Commission.

Clause 40 deems members and employees of the Privacy Commission public servants in terms of the Indian Penal Code, 1860.

Clause 41 requires that the Privacy Commission's offices be located in New Delhi or, if the Chief Privacy Commissioner so directs after consulting with the Central Government, any other place.

Clause 42 permits the Privacy Commission to determine the procedures to be followed by and before it, subject only to the qualification that they comply with the requirements of natural justice. This clause affords the Commission the flexibility to tailor processes to the end of most effectively realizing the object of this legislation.

Clause 43 contains provisions relating to the collection of evidence which are intended to ensure that the Privacy Commission is fully empowered to conduct inquiries effectively. It is equipped with the same powers as would vest in civil courts while trying suits, and is empowered to authorize searches in terms of section 100 of the Code of Criminal Procedure, 1973. Where information is not produced or is produced improperly, sections 175 to 180 and 228 apply.

Clause 44 allows the Privacy Commission to decide matters before it on a majority, and renders these decisions binding. It also empowers the Privacy Commission to direct compliance with this legislation, and to pay compensation or impose penalties in case of non-compliance.

Clause 45 empowers the Privacy Commission with an effective power of enforcement of its decisions under cl. 44, by deeming it to be a civil court under the Code of Criminal Procedure, 1973 and proceedings conducted by it to be judicial proceedings under the Indian Penal Code, 1860.

CHAPTER VI-A

Regulation by Data Controllers and Data Processors

Clause 46 enables data controllers and processors to contribute to the design of the rules and standards that would govern them through public consultations with the Privacy Commission. It is enacted in the awareness that given the rate of technological obsolescence, *inter alia*, ensuring that any code of conduct is current and alive to pragmatic concerns confronted by data controllers and

processors is critical to its effectiveness. In accordance with Clause 47, codes formulated under this clause may not narrow the Privacy Commission's field.

Clause 47 encourages standard-setting around data protection practices by processors and controllers themselves in the form of professional codes. The Privacy Commission will make effective such codes by their registration. In keeping with the objects of this legislation, self-regulatory codes must properly protect personal data in order to be recognized.

Clause 48 provides that the breadth of the Privacy Commission's powers and functions cannot be limited by any code formulated or recognized under this chapter.

CHAPTER VII

Offences and penalties

Clause 49 levies civil penalties for handling data in a manner inconsistent with this legislation. In addition, with a view to deterrence, where a violation of this legislation is accompanied by intent or negligence, criminal liability also accrues. Penalties where sensitive personal data is at issue are enhanced over those that would apply where personal data is involved.

Clause 50 levies civil penalties in all case of contraventions of this legislation in the course of intercepting communications, and creates criminal offences where the contravention is accompanied by intent or negligence, with a view to deterrence.

Clause 51 levies civil penalties in all case of contraventions of this legislation in the course of surveillance, and creates criminal offences where the contravention is accompanied by intent or negligence, with a view to deterrence.

Clause 52 treats abettors as being alike to principal offenders under this chapter.

Clause 53 provides that companies as well as all individuals through whom the offence was committed will be liable for contraventions of this legislation.

Clause 54 provides that offences under this legislation are cognizable and non-bailable, with a view to signaling their seriousness.

Clause 55 makes all non-compliance with this legislation, other than those instances covered by specifically enumerated offences contained within it, liable to civil penalties.

Clause 56 provides that punishments for contraventions of this legislation do not exclude other action in terms of it from being undertaken.

CHAPTER VIII

Miscellaneous

Clause 57 empowers the Central Government to make rules, specifies the matters on which such rules can be made and the duration within which it is to be laid

before Parliament, and saves actions taken under rules that are subsequently modified or annulled before such a modification or annulment.

Clause 58 contains an ouster of the jurisdiction of subordinate courts in disputes arising under the provisions of this legislation.

Clause 59 confers immunity upon the government and the regulator and its officers from civil and criminal liability when they are working this legislation in good faith.

Clause 60 allows the Central Government to make provisions in order to remove any difficulties to putting this legislation into effect for a period of 3 years from its commencement.

Clause 61 contains a *non-obstante* clause that would give the proposed legislation over and above any conflicting others. Exceptions to this rule are contained in Schedule A.

MEMORANDUM REGARDING DELEGATED LEGISLATION

Clause 57 of the Bill empowers the Central Government to make rules for carrying out the purposes of this Bill. As the rules will relate to matters of detail only, the delegation of legislative power is of a normal character.

Source:

[Link to the video:](#)

AS INTRODUCED IN LOK SABHA

Bill No.100 of 2017

THE DATA (PRIVACY AND PROTECTION) BILL, 2017

BY

SHRI BAIJAYANT PANDA, M.P.

ARRANGEMENT OF CLAUSES

CLAUSES

CHAPTER I

PRELIMINARY

1. Short title and commencement.
2. Definitions.
3. Application.

CHAPTER II

RIGHT TO PRIVACY AND DATA PROTECTION

4. Right to privacy.
5. Express consent.
6. Binding determination.
7. Duly informed.
8. Access to personal data.
9. Rectification of personal data.
10. Seeking removal of personal data.
11. Restrict processing.
12. Data portability.
13. Breach of personal data.
14. Legitimate expectation of due diligence.
15. Reasonable restrictions.

CHAPTER III

METHODS AND PRINCIPLES OF DATA COLLECTION AND PROTECTION

16. Collection and processing of data with prior consent.
17. Special provisions for consent in case of minors and persons with disability.
18. Purpose of data collection and processing.
19. Collection or processing of personal data.
20. Special provisions for sensitive personal data.

(ii)

CLAUSES

CHAPTER IV

TRANSFER, STORAGE AND SECURITY OF PERSONAL DATA

21. Prohibition on sharing of personal data.
22. Retention of personal data.
23. Prohibition on storage of personal data.
24. Transfer of personal data to third parties.
25. Cross-border transfer of personal data.
26. Pseudo-anonymisation.
27. Notification of breach.
28. Security protocol.

CHAPTER V

OBLIGATIONS OF DATA CONTROLLER AND DATA PROCESSORS

29. Collection etc.of data in a fair, lawful and transparent.
30. Responsibly of sharing and use of personal data.
31. Fortification of data security.
32. Maintenance of accurate records.
33. Criminal liability.
34. Appointment of Data Protection Officer.
35. Role of Data Protection Officer.

CHAPTER VI

SURVEILLANCE

36. Bar against surveillance.
37. Surveillance by private companies, partnerships or any other body corporate.
38. Surveillance by the State.
39. Duration of surveillance.
40. Security and duty of confidentiality and secrecy.
41. Admissibility in court.
42. No targeted individual profiling.
43. Storage of surveillance.

CHAPTER VII

DATA PRIVACY AND PROTECTION AUTHORITY

44. Constitution of Data Privacy and Protection Authority.
45. Appointment of Chairperson and members to Authority.
46. Constitution of Benches.
47. Terms of office, conditions of service, removal of Chairperson and members.
48. Procedure and powers of the Authority.
49. Functions of the Bench.
50. Filing of complaints.
51. Issuance of orders.

(iii)

CLAUSES

- 52. Appeal.
- 53. Civil Court not to have jurisdiction.

CHAPTER VIII

OFFENCES AND PENALTIES

- 54. Punishment for offences related to personal data.
- 55. Punishment for offences related to Sensitive personal data.
- 56. Breach of confidentiality and security in certain cases.
- 57. Compensation in case of harassment and profiling.
- 58. Penalty for contravention of directions.
- 59. Cognisance.

CHAPTER IX

MISCELLANEOUS

- 60. Protection of action taken in good faith
- 61. Power to remove difficulties
- 62. Overriding effect

SCHEDULE I—EXEMPTIONS

SCHEDULE II—PRIVACY NOTICE

AS INTRODUCED IN LOK SABHA

Bill No. 100 of 2017

THE DATA (PRIVACY AND PROTECTION) BILL, 2017

By

SHRI BAIJAYANT PANDA, M.P.

A

BILL

to codify and safeguard the right to privacy in the digital age and constitute a Data Privacy Authority to protect personal data and for matters connected therewith.

BE it enacted by Parliament in the Sixty-eighth Year of the Republic of India as follows:—

CHAPTER I

PRELIMINARY

5

1. (1) This Act may be called the Data (Privacy and Protection) Act, 2017.

Short title,
extent, and
commencement.

(2) It shall extend to the whole of India and, save as otherwise provided in this Act, it shall also apply to any offence or contravention thereunder committed outside India by any person.

(3) It shall come into force on such date as the Central Government may, by notification in the official Gazette, appoint; and different dates may be appointed for different provisions of this Act and any reference in any such provisions to the commencement of this Act shall be construed as a reference to the commencement of that provision.

5

Definitions.

2. In this Act, unless the context otherwise requires,—

(a) "anonymised data" means data or information processed in such a manner that it no longer relates to an identified or identifiable person;

(b) "Authority" means the Data Privacy and Protection Authority constituted under section 44;

10

(c) "armed force" means any body raised or constituted pursuant to or in connection with, or presently governed by, the Army Act, 1950 (46 of 1950), the Indian Reserve Forces Act, 1888 (4 of 1888), the Territorial Army Act, 1948 (6 of 1948), the Navy Act, 1957 (62 of 1957), the Air Force Act, 1950 (45 of 1950), the Reserve and Auxiliary Air Forces Act, 1952 (62 of 1952), the Coast Guard Act, 1978 (30 of 1978) or the Assam Rifles Act, 2006 (47 of 2006);

15

(d) "authorised officer" means an officer, not below the rank of a Gazetted Officer, of an All India Service or a Central Civil Service, as the case may be, who is empowered by the Central Government, by notification in the Official Gazette, to intercept a communication of another person or carry out surveillance of another person under this Act;

20

(e) "communication" means a word or words, spoken, written or indicated, in any form, manner or language, encrypted or unencrypted, meaningful or otherwise, and includes visual representations of words, ideas, symbols and images, whether transmitted or not transmitted and, if transmitted, irrespective of the medium of transmission;

25

(f) "data" shall for the purpose of this Act refer to data as defined under clause (o) of sub-section (1) of section 2 of the Information Technology Act, 2000;

21 of 2000.

(g) "data controller" means a person who, either alone or jointly or in combination with other persons, determines the purposes for which and the manner in which any personal data are used, or are to be, processed;

30

(h) "data processor" with respect to personal data means any person, apart from an employee of a data controller, who processes data independently or on behalf of a data controller;

(i) "interception" or "intercept" means any activity intended to capture, read, listen to, record and/or copy communication of a person;

35

(j) "intelligence organisation" means institutions set-up under the Intelligence Organisations (Restriction of Rights) Act, 1985, the National Investigation Agency Act, 2008 and/or any other institution set up by the Central Government through an Act of the Parliament or the Executive for the purpose of collection, monitoring, processing and/or analysis of information relevant to national security.

58 of 1985.

34 of 2008.

40

(k) "person" shall for the purpose of this Act refer to an individual:

(l) "personal data" means any data or information which relates to a person if that person can, whether directly or indirectly in conjunction with any other data, be identified from it and includes sensitive personal data;

45

(m) "prescribed" means prescribed by rules made under this Act;

(n) "processing" with respect to data, means obtaining or recording the information or data or carrying out any operation or set of operations on the information or data, whether or not by automatic means, including—

- (i) organisation, adaptation or alteration of the information,
- (ii) or data,
- (iii) retrieval, consultation or use of the information or data,
- (iv) disclosure of the information or data by transmission, dissemination or otherwise making available, or
- (v) alignment, combination, blocking, erasure or destruction of the information or data.
- (o) "pseudo-anonymisation" means processing of personal data in such a manner that the personal data can no longer be attributed to a specific person without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable person;
- (p) "portability" refers to the extent to which data can be moved, copied, transferred or shared by any other means between different computers, computer networks, computer systems, and/or computer resource;
- (q) "profiling" means any form of automated processing of personal data consisting of the use of personal data or information to record and classify behaviour of individuals to predict and analyse their daily activities for purposes other than promotion and marketing of goods and services;
- (r) "surveillance" means any activity intended to collect, watch, monitor, intercept, or enhance the ability to do the same with a view to obtain information about a person, group of persons or class of persons through analysis of any communication, images, signals, data, movement, behaviour or actions;
- (s) "sensitive personal data" means such personal information which consists of information relating to—
- (i) racial or ethnic origins, political or religious views;
 - (ii) passwords;
 - (iii) financial information such as bank account or credit card or debit card or other payment instrument details or financial transactions records;
 - (iv) physical, physiological and mental health condition;
 - (v) sexual activity;
 - (vi) medical records and history;
 - (vii) biometric data relating to the physical, physiological or behavioural characteristics of a natural person which allow their unique identification including, but not limited to, facial images, genetic information, fingerprints, hand prints, foot prints, iris recognition, hand writing, typing dynamics, gait analysis and speech recognition;
 - (viii) any details relating to clauses (i) to (vii) above as provided to body corporates for providing service; and
 - (ix) any of the information received under clauses (i) to (vii) above by body corporates for processing, stored or processed under lawful contract or otherwise;
- Provided that any information that is freely and lawfully available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data for the purposes of this Act; and

22 of 2005 45

(i) "third party" means any person, public authority, agency or any other body other than the person whose data is collected or processed, the controller, the processor, and the persons who, under the authority of the controller or the processor, are authorized to process data or are recipients of the data so processed.

Application.

3. (1) This Act shall apply to—

5

(a) collection, use, storage, disclosure and processing of personal data or information of all persons through wholly or partially automated or manual methods;

(b) data controllers and data processors which are State entities, including Government agencies or authorised personnel on their behalf as well as private companies, partnerships or any other body corporate which conduct activities within the territory of India through a registered place of business or establishment, irrespective of whether data processing is carried out at such place or outside the territory of India; and

10

(c) data controllers and data processors which are State entities, including Government agencies or authorised personnel on their behalf as well as private companies, partnerships or any other body corporate which do not have a registered place of business or establishment in India and offer goods or services to persons in India, irrespective of consideration, as defined under the Indian Contracts Act, 1872, being sought *in lieu* of such goods or services.

15

(2) Nothing in this Act shall apply to collection or processing of data mentioned in Schedule I:

20

Provided that the Central Government may, by notification in the Official Gazette, amend Schedule I by way of addition and deletion of entries thereto :

Provided further that every notification under sub-section (2) shall be issued after consultation with the Authority and shall be laid before each House of Parliament.

25

CHAPTER II

RIGHT TO PRIVACY AND DATA PROTECTION

Right to privacy.

4. Notwithstanding anything contained in any other law for the time being in force, pursuant to article 19 and 21 of the Constitution and subject to the provisions of this Act, all persons shall have a right to privacy.

30

Express consent.

5. (1) No person shall collect, store, process, disclose or otherwise handle any personal data of another person, intercept any communication of another person or carry out surveillance of another person except in accordance with the provisions of this Act.

(2) For the collecting, processing, storing, disclosing and otherwise handling personal data, express and affirmative consent has to be obtained from the requisite person after full disclosure of information as required under Schedule II of this Act.

35

(3) Consent under sub-section (2) shall be considered valid only if it is freely given, specific, informed and an unambiguous indication of a person's intention to allow collecting, processing, storing, disclosing and/or otherwise handling personal data.

(4) Notwithstanding the above, consent may be overridden in cases where there is a legal obligation or medical emergency which is fatal or may likely lead to permanent or irreversible bodily harm as well as the reasonable restrictions mentioned in section 15:

40

Provided that any consent may only be overridden to the extent necessary and the person so affected shall be informed of the same.

Binding determination.

6. For the purposes of section 4, every person shall have the final and binding power to determine the manner in which his personal data is to be dealt with.

45

7. Every person shall be duly informed about the processing of information through issuance of a privacy notice which shall be concise, timely, updated, transparent, intelligible, written in clear and plain language (both English and vernacular language), be easily accessible and provided free of cost to persons with the information specified in Schedule II;

Person to be
duly informed.

Provided that where consent is being sought with regard to a written declaration/online form which contains other clauses and matters, the clauses or portions regarding the privacy notice should be clearly distinguishable from other clauses and matters.

8. Every person shall have access to his personal data which is collected, processed, used or stored by Data Controllers and Data Processors, including the right to obtain a copy and obtain confirmation that his data is being processed along with any supplementary information corresponding to the information mandated under Schedule II of this Act.

Access to
personal data.

9. (I) Every person shall have the right to have his personal data rectified if it is inaccurate or incomplete.

Rectification of
personal data.

15 (2) Every rectification under sub-section (I) shall be carried out by the Data Controller and/or Data Processor in the manner notified by the Central Government in consultation with the Authority as it may deem appropriate:

Provided that every rectification shall be completed within a period of sixty days of receipt of data for rectification.

20 (3) Any person who collects, receives, stores, processes or otherwise handles any personal data of another person shall, to the extent possible, ensure that it is not inaccurate or misleading and, where necessary, is kept up to date.

25 (4) No person who collects, receives, stores, processes or otherwise handles any personal data shall deny, to the person to whom any personal data so collected, received, stored, processed or otherwise handled pertains, the opportunity to review it and, where necessary, rectify anything that is inaccurate, misleading or not up to date.

10. (I) Every person shall have the right to seek removal of personal data from Data Controller—

Seeking removal
of personal data.

30 (a) where personal data is no longer necessary with regard to the purpose for which it was originally collected or processed; or

(b) where the person withdraws consent; or

(c) where personal data has been obtained unlawfully; or

(d) where personal data is required to be erased in accordance with a legal obligation pursuant to a Court order.

35 (2) Notwithstanding anything contained in Sub-section (I), removal of personal data shall not be allowed if there are overriding legitimate interests and it is necessary—

(a) in the interest of fundamental rights;

(b) for compliance of a legal obligation or court order or an any action taken by an officer in exercise of the power vested in him;

40 (c) for establishing or defending a legal claim;

(d) to safeguard public interest.

Illustration

45 If A, a convicted sex offender, seeks removal from the online sex offender registry maintained by the Government, the same shall be disallowed in light of the overriding public interest of safety of women and children.

Restrict processing.	11. (I) During the pendency of consideration of request for removal of specific personal data, the Data Controller and Data Processor shall restrict processing of the specific personal data of the person.	
	(2) It is hereby clarified that sub-clause (I) shall not restrict the collection/storage of personal data.	5
Data portability.	12. Every person shall, as and when required, receive the personal data concerning him, which he has provided to a data controller, in a structured, commonly used and machine-readable format and have the right to data portability to another data controller without any hindrance.	
Breach of personal data.	13. Every person shall have the right to be duly and promptly informed, within seven days about any unauthorized access, destruction, use, processing, storage, modification, de-anonymisation, unauthorized disclosure (either accidental or incidental) or other reasonably foreseeable risks or data security breaches of pertaining to their personal data.	10
Legitimate expectation of due diligence.	14. (I) Every person at the stage of giving consent for collection, processing, use or storage shall have a legitimate expectation that data controllers and data processors shall abide by the provisions of this Act.	15
	(2) Data Controllers and/or Data Processors shall take all security measures necessary for safeguarding and securing the personal data in their custody with due diligence.	
Reasonable restrictions.	15. Notwithstanding anything contained in this Act, the right to privacy shall be restricted by the Authority in the manner specified by this Act for—	20
	(a) reasonable safeguards for sovereignty or integrity of India, national security and for the defence of country;	
	(b) prevention of suspected acts of terrorism, corruption, money laundering, organised crime, sale or purchase of narcotic and psychotropic substances;	
	(c) investigation of cognisable and non-bailable offences under the Indian Penal Code, 1860 after a report has been duly filed under section 154 of the Criminal Procedure Code, 1973;	25 45 of 1860. 2 of 1874.
	(d) investigation of any other offences under the Indian Penal Code, 1860, or any other Act for the time being in force, after an appropriate order has been obtained from the requisite judicial authority with regard to existence of probable cause and providing a fixed time-frame for such collection or processing; and	45 of 1860. 30
	(e) maintenance of public order in situations of imminent danger of breakdown:	
	Provided that the above restrictions must be adequate, relevant, proportionate, not excessive in nature and must be imposed in the manner prescribed.	
Collection and processing, etc. of personal data with prior consent.	CHAPTER III	35
	METHODS AND PRINCIPLES OF DATA COLLECTION AND PROCESSING	
	16. (I) No personal data shall be collected, processed, stored, accessed or monitored without prior express consent of the person directly affected by such act.	
	(2) Consent should be express, affirmative and taken after information as mandated under Schedule II has been provided to the person in a manner which is clearly distinguishable, concise, timely, updated, transparent, intelligible, written in clear and plain language (both English and vernacular language):	40
	Provided that every person subject to data collection shall be duly informed and be provided fair opportunity or mechanism to revoke consent at any time often has consent to the collection of personal data has been obtained:	45

Provided further that where the purpose of processing of data are changed or added or varied in any manner whatsoever, such additional data collection or processing which is in variance of the initial purpose shall not be done without the prior consent of the person.

- (3) It shall be the duty of the data processor or controller to duly provide information and adequate explanation to the person while taking consent about the manner and extent to which personal data shall be accessed, collected, stored or processed.

Explanation.—For the purposes of this section "consent" shall have the same meaning and safeguards as provided under the Indian Contracts Act, 1872.

- 17.** (I) Notwithstanding anything contained in section 16, where the personal data belongs to a minor as per the Indian Majority Act 1875, the consent of minor shall be—

- (a) obtained from a legal guardian; and
- (b) duly verified by the data controllers and processors:

Special provisions for consent in case of minors and persons with disability.

Provided that upon attaining majority, the minor shall have the right to either continue or terminate the consent given by the legal guardian on his behalf.

- (2) In the case of differently abled persons, the data controllers and data processors shall make special provisions for providing privacy notices and obtaining consent in accordance with accepted standards and as per directions of the Authority.

- 18.**(I) Every data controller and data processor must duly notify every person of the purpose for which data is collected, accessed or processed in a comprehensive format and with the adequate information as provided under Schedule II of the Act:

Purpose of data collection and processing.

Provided that in case of multiple purposes, each purpose shall be displayed separately and the ramifications thereof shall be provided to the person at the time of taking his consent.

- (2) No personal data shall be collected, accessed or processed unless deemed necessary for achievement of the purpose specified under sub-section (I) and connected to the stated function:

Provided that if any other personal data is collected it shall be marked as "optional".

- (3) Any additional or further processing of personal data for archiving or scientific or historical or statistical research, shall not be considered incompatible with the initial purpose if it is,—

- (a) bona fide;
- (b) in public interest; and
- (c) subject to adequate safeguards.

- 19.** Personal data of a person with his consent may be collected or processed lawfully, if—

Collection or processing of personal data.

(a) necessary for performance of a contract or at a stage immediately prior to entering into a contract;

(b) required in furtherance of a legal obligation;

(c) in case of a person's medical emergency;

(d) necessary for administration of justice pursuant to a court order;

(e) required for performance of any statutory, governmental or other functions by data processor or controller as duly specified to the person subject to data collection;

(f) necessary for the legitimate interests pursued by data controller or processor or the third party to whom data is disclosed after it is duly informed to the person:

Provided that the interests of data processors or controller or third parties shall be adequately balanced against any prejudicial effect of the same on the rights and freedoms of the person as guaranteed under this Act and under the Constitution of India; and

(g) required for any other purpose as may be notified by the Central Government 5 in consultation with the Authority, from time to time.

20. Notwithstanding anything contained in section 16 or section 19 of this Act,

(1) Sensitive personal data shall not be processed unless express, affirmative and explicit written consent of the person subject to data collection has been obtained through letter or fax or email from the said person. 10

(2) No sensitive personal data under sub-section (1) shall be processed for any purpose apart from for the specific purpose for which it was collected and/or implementation of welfare schemes and social protection laws.

(3) If sensitive personal data has been collected by various government agencies, institutions, authorities or private companies, partnerships or any other body corporate. 15 for a specific purpose or as a part of a statutory or legal requirement and any form of collaborating, converging or monitoring between or individually by entities shall be expressly barred if it amounts to or reasonably lead to —

(a) individual profiling except for circumstances of reasonable restriction as mentioned under section 15 of this Act; or 20

(b) mass profiling or profiling of certain group or class of persons without any lawful reason or adequate basis; or

(c) unlawful access by third parties.

(4) It shall be the duty of the data controller or processor, as the case may be, to ensure that the sensitive personal data is collected, stored or processed, in accordance 25 with this Act with reasonable advanced security measures and safeguards to ensure the safety of such data.

CHAPTER IV

TRANSFER, STORAGE AND SECURITY OF PERSONAL DATA

Prohibition
on sharing of
personal data.

21. No personal data shall be shared in contravention of the provisions of this Act. 30

Retention of
personal data.

22. No personal data shall be retained after the achievement of purpose for which it was collected and has been duly completed up to the satisfaction of all parties:

Provided that nothing in this section shall apply to databases of sensitive personal data duly established by the Central Government or State Government, as the case may be.

Prohibition on
prolonged or
unnecessary
storage of
personal data.

23. (I) No person shall store any personal data of another person for a period longer than is necessary to achieve the purpose for which it was collected or received, or, if that purpose is achieved or ceases to exist for any reason, for any period following such achievement or cessation. 35

(2) Save as provided in sub-section (3), any personal data collected or received in relation to the achievement of a purpose shall, if that purpose is achieved or ceases to exist for any reason, be destroyed forthwith. 40

(3) Notwithstanding anything contained in this section, any personal data may be stored for a period longer than is necessary to achieve the purpose for which it was collected or received, or, if that purpose has been achieved or ceases to exist for any reason, for any period following such achievement or cessation, if — 45

(a) the person to whom it pertains grants his consent to such storage prior to the purpose for which it was collected or received being achieved or ceasing to exist; or

5 (b) it is required to be stored for historical, statistical or research purposes under the provisions of an Act of Parliament:

Provided that only that amount of personal data that is necessary to achieve the purpose of storage under this sub-section shall be stored and any personal data that is not required to be stored for such purpose shall be destroyed forthwith.

24. Any transfer of personal data to a third party shall be done pursuant to taking express, affirmative consent under Section 16 of this Act and after adequately informing them of the ramifications thereof in a comprehensive manner the requirements specified under Section 7 of this Act:

10 Provided that any transfer of data to third parties shall be done only after ensuring that the third parties' privacy policies and security standards are in no way less privacy preserving than that of the transferring party.

Transfer of personal data to third parties.

25. Any cross border transfer of personal data shall be done pursuant to taking express, affirmative consent under Section 16 of this Act and after adequately informing them of the ramifications thereof in a comprehensive manner the requirements specified under Section 7 of this Act:

Cross-border transfer of personal data.

20 Provided that any cross border transfer of data to any entity or person outside the territory of India shall be done only after ensuring that the privacy policies and security standards followed by such entity are in no way less privacy preserving than those prescribed under this Act.

25. For collecting, processing, storing, disclosing and/or otherwise handling personal data, pseudo - anonymisation shall be encouraged as far as possible.

Pseudo-anonymisation.

27. It shall be the duty of the data controller and data processor, as the case may be, in case of any breach, unauthorized access, destruction, use, processing, storage, modification, de-anonymisation, unauthorized disclosure (either accidental or incidental), or other reasonably foreseeable risks of personal data, to notify to the person who is the 30 subject of such personal data as well as the Authority and take adequate steps to mitigate any harm or damage of the data security breach within seven days.

Notification of breach.

28. It shall be the duty of the data controller and processor, as the case may be, to maintain adequate security measures and safeguards in accordance with the nature and form of security protocol as notified by the Central Government in consultation with the 35 Authority, from time to time.

Security protocol.

CHAPTER V

OBLIGATIONS OF DATA CONTROLLER AND PROCESSORS

29. (1) It shall be the duty of the data controller or processor, as the case may be to collect, store, access or process the personal data in a fair, lawful and transparent manner 40 and in compliance with the provisions of this Act.

Collection, etc. of data in a fair, lawful and transparent.

(2) Any personal data obtained in contravention of sub-section (1) shall be deemed to be unlawfully obtained.

30. It shall be the duty of the data controller or processor or third party, as the case may be, to ensure that all personal data is reasonably shared only when it is necessary, 45 while maintaining confidentiality and in compliance with the provisions of this Act.

Responsibility of sharing and use of personal data.

31. It shall be the duty of the data controller or processor or third party, as the case may be, to take adequate measure for fortification of data security against unauthorised or unlawful access or use, accidental loss, damage, or any form of cyber-attacks:

Fortification of data security.

Provided that in the case of a breach of data, it is the duty of the data controller or processor or third party to notify the affected persons within seven days of the occurrence of the breach as well as take adequate measures to mitigate any harm or damage:

Provided further that the burden of proof to substantiate that adequate measures are in accordance with the provisions of this Act, shall lie on the data controller or processor 5 or third party, as the case may be.

Maintenance of accurate records.

32. It shall be the duty of the data controller or processor or third party, as the case may be, to maintain accurate records of data collected, accessed, stored and processed along with record of consent obtained as per the provisions of this Act.

Criminal liability.

33. Where a data controller or data processor or third party, as the case may be, has 10 committed an offence under Chapter 8 which is punishable with imprisonment, every person in-charge of and responsible for the conduct of business shall, irrespective of direct commercial or financial benefit, incur criminal liability and be punished accordingly:

Provided that nothing contained in this Section shall render any such person in-charge liable to any punishment, if he proves to the satisfaction of the Authority that such offence was committed without his knowledge or that he had exercised all due diligence 15 to prevent the commission of such offence.

Appointment of Data Protection Officer.

34. (1) Every data controller or processor or third party, as the case may be, shall appoint a Data Protection Officer having adequate technical expertise in the field of data collection or processing and the ability to address any requests, clarifications or complaints 20 made with regard to the provisions of this Act:

Provided that the data controllers and processors employing less than live hundred people and having a per capita turnover of less than one crore rupees may jointly appoint a Data Protection Officer, for resolving or addressing any requests, clarifications or complaints made herein in collaboration with other bodies with similar size or turnover. 25

(2) No additional fee shall be charged for resolving or addressing any requests, clarifications or complaints made herein.

Role of Data Protection Officer.

35. (1) The Data Protection Officer shall—

(a) act as an independent person;

(b) address requests, clarifications or complaints made in writing, including 30 through electronic form, by any aggrieved person or legal representative thereof;

(c) take steps to initiate an inquiry and commence proceedings within seven days of receiving the complaint;

(d) resolve the matter within ninety days of receipt of complaint;

(e) recommend the data controller or processor to take action; and 35

(f) record the proceedings, the results thereof and the reasons for arriving at the decision in writing.

(2) In cases where the Data Protection Officer has not been appointed or is unable to or does not adequately resolve the complaints within the stipulated period of ninety days, the complainant may approach the Data Privacy Authority for redressal of complaints. 40

CHAPTER VI

SURVEILLANCE

Bar against surveillance.

36. Except for the manner provided in this Act and the rules prescribed thereto, no person shall conduct or assist in conducting any surveillance of another person.

- 37.** Any person except a public servant or authority duly authorised by the Central Government to order or conduct surveillance or to assist in pending investigation by the competent authority shall be expressly barred from initiating, assisting, conducting or abetting any act of surveillance under this Act. Surveillance by private companies, partnerships or any other body corporate.
- 5 **38. (1)** The State has the power to collect, process, monitor and intercept personal data in accordance to the reasonable restrictions provided under section 15. Surveillance by the State.
- (2) Any officer authorised by the Central Government, on the basis of information received or lawfully discovered by police, armed forces, intelligence organisation or any public official, if satisfied that the information sets out a reasonable threat to sovereignty, 10 integrity, national security or defence of public order, he may forward the same to the concerned intelligence organisations.
- (3) The concerned intelligence organisation shall, on receipt of information mentioned under sub-section (2), if deem necessary, seek an order from the Authority who may either reject or issue an order allowing surveillance or interception of personal 15 data for reasons recorded in writing and addressed to concerned organisation:
- Provided that the every case referred to the Authority under this section shall be processed and an appropriate order shall be passed within a period of sixty days of receipt of the case:
- Provided further that the order should specify the communications or class of 20 communications to or from the persons or class of persons that shall be subject to the order.
- (4) For the purpose of sub-section (2), a Special division shall be set up by the Central Government for assistance of the Authority for determination of the cases referred:
- Provided that prior to issuing the order, the Authority shall satisfy itself that all other 25 lawful means to acquire the information sought to be intercepted has been exhausted and that the proposed interception is reasonable, proportionate and not excessive.
- (5) The Special division set up under section (4) shall have the power to conduct preliminary investigation in the manner as prescribed by the Central Government, from time to time, submit their findings to the Authority who shall thereafter issue a detailed 30 order to the intelligence organisation:
- Provided that in case of military intelligence, which appears to be inaccessible or sensitive and/or confidential, the Authority shall consult the Cabinet Secretary, Government of India for the purposes of issuance of order under this section.
- (6) After, receipt of order from the Authority the intelligence organisation shall 35 conduct surveillance in accordance to the express conditions provided in the order.
- 39.** Every order issued under section 38 shall specify the time period for carrying out the surveillance by the intelligence organisation of the personal data: Duration of surveillance.
- Provided that if any extension is required for the surveillance, the intelligence organisation shall approach the Authority along with reasons for such extension.
- 40 **40.** Every State authority, intelligence organisation or private companies, partnerships or any other body corporate shall, as the case may be, which participate, assist, co-operate, conduct or carry out activity to facilitate surveillance pursuant to provisions of this chapter, take reasonable steps to ensure security of the data so collected and maintain the confidentiality and secrecy thereof. Security and duty of confidentiality and secrecy.
- 45 **41.** If at any stage, information or personal data obtained through surveillance is required to be produced in a court of law, the onus to prove that the same has been collected in accordance with the provisions of this Act while maintaining a proper chain of custody Admissibility in court.

without any tampering or external interference shall be on the concerned State authority, intelligence organisation or private entity, as the case may be.

No targeted individual profiling.

42. Any targeted profiling of individuals or of a certain section or class of persons without any basis and harassment, whether physical or financial or other means, shall be expressly barred and be deemed as violation of privacy under this Act. 5

Storage of surveillance.

43. No information or personal data that is collected in the process of surveillance which is not relevant for the purposes of evidence or for continuing investigation by the intelligence organisations shall not be stored by or accessible to the intelligence organisations after a period of expiry of one year from the date on which the order under which the information was obtained. 10

CHAPTER VII

DATA PRIVACY AUTHORITY

Constitution of Data Privacy Authority.

44. The Central Government shall, by notification in the Official Gazette, constitute an Authority to be known as the Data Privacy and Protection Authority for carrying out the purposes of this Act in such manner as may be prescribed. 15

Appointment of Chairperson and other members to the Authority.

45. (1) The Central Government shall, in consultation with the Chief Justice of India, appoint a Chairperson and other members to the Authority in such manner as may be prescribed.

(2) The Authority shall constitute of judicial members as well as technical members in equal proportion. 20

(3) A judicial member shall otherwise be qualified to be a High Court Judge or have been a member of the Indian Legal Services and have held a post in Grade I of that Service for at least three years.

(4) A technical member shall have expertise, special knowledge of and adequate professional experience in technology and processing/collection of data. 25

(5) The Chairperson of the Authority shall be the senior-most judicial member.

Constitution of Benches.

46. (1) Subject to the provisions of this Act, the Authority may, by notification in the Official Gazette, constitute Benches to exercise the jurisdiction, powers and authority conferred to under this Act.

(2) Each Bench shall consist of at least one judicial and one technical member of the Authority to be decided by Chairperson in such manner as may be prescribed. 30

(3) The Benches of the Authority shall sit at New Delhi and at such other places as the Central Government may, in consultation with the Chairperson of the Authority, by notification in the Official Gazette, specify.

(4) The Central Government shall, by notification in the Official Gazette, specify 35 the areas in relation to which each Bench of the Authority may exercise its territorial jurisdiction.

(5) Notwithstanding anything contained in sub-section (3), the Chairperson of the Authority may transfer a member from one Bench to another Bench for carrying out the purposes of this Act in such manner as may be prescribed. 40

(6) If at any stage of the hearing of any case or matter it appears to the Chairperson or a member of the Authority that the case or matter is of such a nature that it ought to be heard by a Bench consisting of more members, the case or matter may be transferred by the Chairperson to such Bench as the Chairperson may deem fit.

47. (1) The Chairperson and every member of the Authority shall hold office for a period of five years or till the age of sixty-five years whichever is earlier:

Provided that no member shall be elected for more than two consecutive terms.

(2) The Central Government shall remove a person from the office of Chairperson or 5 member, as the case may be, if that person—

(i) has been adjudged as insolvent;

(ii) has been convicted of an offence of moral turpitude or any other offence as may be deemed appropriate and notified by the Central Government;

(iii) has become physically or mentally incapable of acting as a member;

10 (iv) has acquired such financial or other interest as is likely to prejudicially affect completion of duties;

(v) has abused his position in such a manner that continuance in office shall be prejudicial to public interest:

15 Provided that no person shall be removed under this sub-section unless he has been given a reasonable opportunity of being heard in the matter.

(3) The salary and allowances payable to and other terms and conditions of service of Chairperson and members of the Authority shall be such as may be prescribed.

48. (1) The Authority shall not be bound by the procedure laid down by the Code of 5 of 1908. Civil Procedure, 1908, but shall be guided by the principles of natural justice and, subject to 20 the other provisions of this Act and of any rules.

(2) The Authority shall have power to regulate its own procedure including the place at which it shall have its sittings.

5 of 1908. (3) The Authority shall have, for the purposes of discharging its functions under this 25 Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely:

(a) summoning and enforcing the attendance of any person and examining him on oath;

(b) requiring the discovery and production of documents or other electronic records;

30 (c) receiving evidence on affidavits;

(d) issuing commissions for the examination of witnesses or documents;

(e) calling upon any data processor or data controller at any time to furnish in writing such information or explanation as may be deemed necessary;

35 (f) hearing and deciding matters where criminal liability is involved with respect to the provisions of this Act;

(g) issuing an order for search and seizure pursuant to a complaint or *suo-moto* if there is *prima facie* evidence of contravention or violation of this Act;

(h) reviewing its decisions;

(i) dismissing an application for default or deciding it *ex parte*; and

40 (j) any other matter which may be prescribed.

45 of 1860. (4) Every proceeding before the Authority shall be deemed to be a judicial proceeding 2 of 1974. within the meaning of Sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code, 1860 and the Authority shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

Terms of office, conditions of service, removal of Chairperson and members.

Procedure and Powers of the Authority.

Functions of the Bench.

49. The Authority shall,—

- (a) adjudicate all disputes and contraventions of the provisions of this Act referred to it, impose penalties and punishments thereof;
- (b) study and undertake impact assessment of Bills tabled before each House of Parliament, existing legislation, ordinances and rules pertaining to the subject matter of this Act as it deems necessary and make recommendations to the concerned Ministry; 5
- (c) consult with stakeholders on any issues pertaining to the subject matter of this Act which are of public importance;
- (d) consult with the Central Government according to the provisions of this Act; 10 and
- (e) *suo-moto* initiate inspection of **Data Controllers and Data Processors** to assess compliance with the provisions of this Act.

Filing of Complaints.

50. Any person aggrieved by the decision of the Data Protection Officer or not received any adjudication despite lapse of ninety days may file a written complaint with 15 regard to non-compliance, contravention or any other violation of this Act before the Authority:

Provided that where the Data Protection Officer is not appointed, the person may directly approach the Authority.

Issuance of orders.

51. The Bench shall upon adjudicating the complaints referred to in section 50 award 20 fines, call for directive or injunctive measures, compensation and/or imprisonment of such term as it may deem appropriate.

Appeal.

52. An appeal against the decision of the Bench shall lie to the Telecom Disputes Settlement Appellate Tribunal set up in accordance with the provisions of the Telecom Regulatory Authority Act, 1997.

25 24 of 1997.

Civil Court not to have Jurisdiction.

53. No civil court have jurisdiction to entertain any suit or proceedings in respect of any matter dealt with under the provisions of this Act.

Punishment for offences related to personal data.

54. Whoever, except in compliance with the provisions of this Act, collects, stores, receives, processes, publishes or otherwise handles personal data shall be punishable with 30 a term of imprisonment for a term which may extend up to five years and fine which may extend up to rupees fifty thousand for each day of unlawful access to the personal data:

Provided that where any offence under this Act has been committed by a company and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any neglect on the part of any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall be deemed to be guilty of that offence, and shall be liable to be proceeded against and punished accordingly. 35

Punishment for offences related to sensitive personal data.

55. Whoever, except in compliance with the provisions of this Act, collects, stores, receives, processes, publishes or otherwise handles sensitive personal data shall be 40 punishable with a term of imprisonment which may extend up to ten years and fine which may extend up to rupees one lakh for each day of unlawful access to the personal data and shall also be required to provide adequate compensation to the person whose sensitive personal data has been breached to be determined by the Authority in such manner as may be prescribed.

45

	56. Whoever breaches confidentiality or compromises security of any personal data being collected as a part of surveillance authorised under this Act shall be liable to be punished with a term of imprisonment which may extend up to ten years and/or fine which may extend up to rupees fifty thousand for each day of said breach.	Breach of confidentiality and security in certain cases.
5	57. Whoever has been victim of profiling and harassment, whether physical or financial under section 42 shall be entitled to adequate compensation for financial loss and mental trauma in such manner as may be prescribed.	Compensation in case of harassment and profiling.
10	58. Any wilful non-compliance of a direction or order of the Bench shall be punishable with imprisonment for a term which may extend upto six month and fine which may extend upto rupees fifty thousand for each day of said breach.	Penalty for contravention of directions.
2 of 1974.	59. Notwithstanding anything contained in the Code of Criminal Procedure, 1973, the offences under this chapter shall be treated as cognizable.	Cognizance.
	CHAPTER IX MISCELLANEOUS	
15	60. No suit or other legal proceeding shall lie against the Central Government, State Government, Chairperson or Member of the Authority, or any person acting under the direction either of the Central Government, State Government, Chairperson or Member of the Authority, as the case may be, in respect of anything which is in good faith done or intended to be done in pursuance of this Act or of any rules or any order made thereunder.	Protection of action taken in good faith.
20	61. If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order, published in the Official Gazette, make such provisions, not inconsistent with the provisions of this Act, as appears to it to be necessary or expedient for removing the difficulty:	Power to remove difficulties.
25	Provided that no such order shall be made under this section after the expiry of a period of three years from the commencement of this Act.	
24 of 1997. 21 of 2000.	62. The provisions of this Act shall have overriding effect over the Telecom Regulatory Authority Act, 1997 the Information Technology Act, 2000 or any other legislation pertaining to collection, processing, interception and monitoring of personal data.	Overriding effect.
30	63. (1) The Central Government may, by notification in the Official Gazette, make rules for carrying out the purposes of this Act.	Power to make rules.
35	(2) Every rule made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or both the Houses agree that the rule should not be made, the rule shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule.	

SCHEDULE I

[See Section 3(2)]

EXCEPTIONS

This Act shall not apply to collection or processing of data which falls within the following categories—

1. purely for personal reasons or pertaining to household activities;
2. of a deceased person;
3. eligible to be disclosed under the Right to Information Act, 2005; and
4. that is anonymised and cannot be used to identify the natural person.

SCHEDULE II

[See section 3]

PRIVACY NOTICE

Any privacy notice published under this Act must contain the following ingredients—

(a) What personal data or information is being collected;

(b) the purposes of the processing;

(c) the categories of personal data concerned;

(d) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations along with the safeguards thereof;

(e) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(f) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(g) the right to lodge a complaint with the competent authority;

(h) where the personal data are not collected from person, any available information as to their source.

(i) the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the person.

STATEMENT OF OBJECTS AND REASONS

While right to life and personal liberty are granted under article 21 of the Constitution of India, our jurisprudence, judicial pronouncements and case laws have extended it to encompass *inter alia*, a life of dignity. However, there is no express statutory grant of right to privacy.

The Hon'ble Supreme Court has recognised the right to privacy in a limited and reasonable manner with the landmark case of *Kharak Singh v. The State of U.P.* It has further expounded on the principle and safeguards thereof in various landmark cases such as *PUCL v. Union of India* and *Selvi v. Union of India*, delineating the extent of the right to privacy in communications and the right to withhold consent to certain privacy violations, respectively.

With the increased proliferation of technology in daily lives, it is becoming increasingly important for us to recognise and implement a meaningful right to privacy as also recognised by the Special Rapporteur on the Right to Privacy, Office of the High Commissioner for Human Rights. Further, India has globally, as a party to the Universal Declaration of Human Rights (UDHR), and the International Covenant for Civil and Political Rights (ICCPR), acknowledged the right to privacy as an universal human right under Article 12 of the UDHR and Article 17 of the ICCPR.

On one hand, there is significant success of Aadhaar, which is the largest biometric database in the world, as a means to implement social welfare schemes and serves as a tool for financial inclusion. On the other hand, there is reasonable apprehension as to the security of the information contained in the database and during any information transmission as a part thereof.

Today, personal data is being collected and processed at a much larger scale that is not limited to AADHAAR; every application and website we use collects and processes our personal data. Our personal data is vulnerable to any non-State actor, private entity around the globe with the technological know-how to access and process this data unlawfully. It may be utilised by Non-State Actors to target Indian citizens through cyber-attacks for financial gains as well as to profile the interests of any person. Ready availability and accessibility of personal data can also assist terror groups or religiously extreme groups in profiling, propagating extremist ideology and preying on young, poor and destitute.

The present Bill is an effort to avoid situations like a country-wide hack like in the case of Estonia in 2007 and the recent global ransomware attack 'WannaCry' in 2017. Globally, data is being considered the new oil and in the coming years, our international trade and economic relations will depend on the health and bargaining power of our data economy. Hence it is timely to address the issue on data protection and protect the privacy of all persons. It intends to provide rights of persons *vis-a-vis* their own information, as well as procedures for data collection, data processing, reasonable and targeted surveillance, and means of redress in case of breaches and violations.

In light of this, while the collection and processing of data is important, there is an overwhelming need to secure personal data and ensure better security by creating a statutory obligation to safeguard data and individuals. To that effect, this Bill seeks to establish *Inter alia*, a balance between rights of individuals and legitimate intervention by the State.

The Bill seeks to codify and safeguard the right to privacy for all juristic persons in the digital age, balanced with the need for data protection in the interests of national security.

Hence this Bill.

NEW DELHI;
April 7, 2017

BAIJAYANT PANDA

FINANCIAL MEMORANDUM

Clause 34 of the Bill provides for appointment of Data Protection Officer. Clause 44 provides for establishment of the Data Privacy Authority for carrying out the purposes of this Act. Clause 45 provides for the appointment of a Chairperson and other members to the Authority. Clause 46 provides for constitution of Benches by the Authority. The Bill, therefore, if enacted would involve expenditure from the Consolidated Fund of India. It is estimated that a sum of about rupees ten crores would involve as recurring expenditure per annum from the Consolidated Fund of India.

A non-recurring expenditure of about rupees fifty crores is also likely to be involved out of the Consolidated Fund of India.

MEMORANDUM REGARDING DELEGATED LEGISLATION

Clause 63 of the Bill empowers the Central Government to make rules for carrying out the purposes of the Act. As the rules will relate to matters of detail only, the delegation of legislative power is of a normal character.

LOK SABHA

A

BILL

to codify and safeguard the right to privacy in the digital age and
constitute a Data Privacy Authority to protect personal data
and for matters connected therewith.

(*Shri Baijayant Panda, M.P.*)

Save Our Privacy | Bill

THE PERSONAL DATA AND INFORMATION PRIVACY CODE BILL, 2019

A Bill

to establish an effective regime to protect, promote and fulfil the fundamental right to privacy of all natural persons and protect personal data concerning them, to set out conditions upon which surveillance of natural persons and interception of communications may be carried out, to constitute a Privacy Commission, and for matters connected therewith or incidental thereto.

WHEREAS the right to privacy is an inalienable fundamental right of all natural persons indispensable to the preservation of human dignity, personal autonomy and the exercise of constitutional liberties;

AND WHEREAS the need to protect privacy has only increased in the digital age, with the emergence technologies such of big data analytics;

AND WHEREAS the delivery of goods and provision of services often entails the collection, storage, processing and disclosure, including international transfers of personal data;

AND WHEREAS good governance requires that all interception of communications and surveillance must be conducted with due process strictly in accordance with law, in consonance with the rights to freedoms and privacy under Part III of the Constitution and only upon establishing the need for the same;

AND WHEREAS it is necessary to harmonise any conflicting interests and competing legislation;

NOW, THEREFORE, it is expedient to provide for an enforceable means to protect the informational privacy of natural persons.

BE it enacted by Parliament in the Seventieth Year of the Republic of India as follow:—

CHAPTER I

PRELIMINARY

Short title, extent and commencement.

1. (1) This Act may be called the Personal Data and Information Privacy Code Act, 2019.
(2) It extends to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention hereunder committed outside India by any person, wherever located.

(3) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint.

Definitions

1. (1) In this Act unless the context otherwise requires,—
 - (a) “aggregate”, with its grammatical variations and cognate expressions, in relation to personal data, means adding, removing, filtering, mixing, combining or recombining records of data;
 - (b) “anonymise” means, in relation to personal data, the irreversible removal or alteration of all data that may, whether directly or indirectly in conjunction with any other data, be used to identify a natural person or data subject;
 - (c) “appropriate Government” means, in relation to the Central Government or a Union territory Administration, the Central Government; in relation to a State Government, that State Government; and, in relation to a public authority which is established, constituted, owned, controlled or substantially financed by funds provided directly or indirectly:—
 - (i) by the Central Government or a Union territory Administration, the Central Government;
 - (ii) by a State Government, that State Government;
 - (d) “authorised officer” means an officer of a competent organization, not below the rank of a Gazetted Officer of an All India Service or a Central Civil Service, as the case may be, who is empowered by the Central Government, by notification in the Official Gazette, to intercept the communications of another person or carry out any surveillance of another person under this Act;
 - (e) “biometric data” means any data relating to the physical, physiological or behavioural characteristics of a natural person which allows the verification or authentication of that person’s identity including, but not restricted to, facial images, fingerprints, hand prints, foot prints, iris recognition, handwriting, typing dynamics, gait analysis and speech recognition;
 - (f) “Chief Privacy Commissioner” and “Privacy Commissioner” mean the Chief Privacy Commissioner and Privacy Commissioners appointed under section 48;
 - (g) “collect”, with its grammatical variations and cognate expressions, means, in relation to personal data, any action or activity that results in a person obtaining, or coming into the knowledge or possession of, any personal data of another person, whether directly or indirectly;
 - (h) “communication” means a word, signs, gestures, spoken, written or indicated, in any form, manner or language, encrypted or unencrypted,

meaningful or otherwise, and includes visual representations of words, ideas, symbols and images, and the metadata in relation whether transmitted or not transmitted and, if transmitted, irrespective of the medium of transmission;

(i) “competent organisation” means an organisation authorised by an Act of Parliament to carry out surveillance and/or interception, and includes a public authority as listed in the Schedule.

(j) “consent” means it is free, informed and unambiguous indication of a data subject’s agreement;

(k) “data” means shall have some meaning as assigned in it section 2(o) of the Information Technology Act, 2000;

(l) “data controller” means any person including appropriate Government who, either alone, or jointly, or in concert with other persons, determines the purposes for which and the manner in which any personal data is processed;

(m) “data processor” means any person including appropriate Government who processes any personal data on behalf of a data controller;

(n) “data subject” means a natural person who is a citizen under the Citizenship Act, 1955 or who has resided in India for a period of one hundred and eighty two days or more in the twelve months preceding the previous year.

(o) “deoxyribonucleic acid data” means all information, of whatever type, concerning the characteristics of a natural person that are inherited or acquired during early prenatal development;

(p) “destroy”, with its grammatical variations and cognate expressions, means, in relation to personal data, to cease the existence of, by deletion, erasure or otherwise, any personal data which becomes irretrievable in whole or in part, including information about the existence of such data itself;

(q) “disclose”, with its grammatical variations and cognate expressions, means, in relation to personal data, any action or activity that results in a person coming into the knowledge or possession of any personal data of another person;

(r) “interception” or “intercept” means any activity intended to capture, read, listen to or understand the communication of a person;

(s) “officer-in-charge of a police station” shall have the meaning ascribed to it under clause (o) of section 2 of the Code of Criminal Procedure, 1973;

(t) “person” includes a natural person or legal person including a company, a firm, an association of persons, a public authority or a body of individuals, wherever located, whether incorporated or not;

(u) “personal data” means any data which relates to a natural person if that person can, whether directly or indirectly in conjunction with any other data, be identified or identifiable from it and includes sensitive personal data:

Provided that the term “personal data” shall not include data which is a matter of public record except details of victims in cases of sexual assault, kidnapping or abduction.

(v) “prescribed” means prescribed by rules and regulations made under this Act;

(w) “Privacy Commission” means the body constituted under sub-section (1) of section 47;

(x) “Privacy Officer” means the Privacy Officer designated under sub-section (3) of section 36 and sub-sections (3) and (4) of section 43;

(y) “process”, with its grammatical variations and cognate expressions, means, in relation to personal data, any action or operation which is performed upon personal data of another person, whether or not by automated means including, but not restricted to, collection, aggregation, organisation, structuring, adaptation, modification, retrieval, consultation, use, alignment or destruction;

(z) “public authority” shall have the meaning assigned to it under clause (h) of section 2 of the Right to Information Act, 2005;

(za) “receive”, with its grammatical variations and cognate expressions, means, in relation to personal data, to come into the knowledge or possession of any personal data of another person;

(zb) “sensitive personal data” means data or metadata as to a person’s—

(i) biometric data;

(ii) deoxyribonucleic acid data;

(iii) identification number, or any identity attributes;

(iv) location data;

(v) sexual preferences and practices;

(vi) medical history and health information;

(vii) political affiliation or opinions;

(viii) present and past membership of a political, cultural, social organisations including but not limited to a trade union as defined under section 2(h) of the Trade Union Act, 1926;

(ix) ethnicity, religion, race or caste; and

- (x) financial and credit information, including financial history and transactions except in cases of public officials or when such information is considered as a public record or its disclosure is made under any law.
- (zc) "State Privacy Commission" means the body constituted under sub-section (1) of section 65;
- (zd) "Surveillance and Interception Review Division" means the bodies constituted under sub-section (1) of section 70;
- (ze) "store", with its grammatical variations and cognate expressions, means, in relation to personal data, to retain, in any form or manner and for any purpose or reason, any personal data of another person;
- (zf) "surveillance" means any activity, directly or indirectly intended to watch, monitor, record or collect, or to enhance the ability to watch, record or collect, any information, images, signals, data, movement, behaviour or actions, of a person, a group of persons, a place or an object, for the purpose of obtaining information about a person and their private affairs, including:
- (i) directed surveillance that is covert surveillance undertaken for a specific investigation or operation even if the person surveilled was not specifically identified in relation to the surveillance operation;
 - (ii) inclusive surveillance which is covert surveillance carried out by an individual or surveillance device in relation to anything taking place in any private premises or private vehicle;
 - (ii) covert human intelligence gathering which is information obtained by a person who establishes or maintains a personal or other relationship with a person for a covert purpose of using it to obtain access to any personal information about that individual;
 - (iv) surveillance undertaken through installation and use of CCTV and other system which capture audio-visual information to identify or monitor individuals; but does not include collection of personal data under sections 7, 11 and 12.
2. All other words expressions used herein but not defined and defined in the General Clauses Act, 1897 or the Code of Criminal Procedure, 1973 as the case may be, shall have the same meanings as assigned to them in those Acts.

Chapter II

Right to Privacy

Principles applicable to protecting privacy- In exercising the powers conferred by this Act, regard shall be had to the following consider-

ations, namely:—

1. that the right to privacy is a fundamental right essential to the maintenance of a democratic, open society and is recognised as a fundamental human right mentioned in Part III of the Constitution and in international treaties to which India is a party;
- (2) that personal data with its attributes belongs solely to the natural person to whom it pertains who are referred to as the data subjects for the purposes of this Act;
- (3) that personal data of data subjects shall be processed fairly and lawfully and in no circumstance shall be processed unless the conditions under this Act are met and subject to conditions under this Act are fulfilled;
- (4) that intrusions into privacy shall, be for lawful purposes, measured by principles of legality, necessity and proportionality;
- (5) that unless as otherwise expressly provided the consent of data subject for a specific purpose shall be a mandatory condition prior to storage and processing of his personal data;
- (6) that personal data is required by data controllers, and data processors, to enable good governance and the delivery of goods and provision of services without undue delay which may be provided by a meaningful, revocable and accountable notice and consent framework;
- (7) that the right to privacy shall not be used to limit or fetter the fundamental right to freedom of speech and expression of journalists and the press or accountability of the Government and public institutions under the Right to Information Laws;
- (8) that privacy shall be upheld by a statutory body which is independent, impartial, well resourced and free from influence and extraneous pressure.

Right to privacy.

1. Without prejudice to the generality of the provisions contained herein, all natural persons shall have a right to privacy which shall be implemented as per principles laid down in section 3.
- (2) For the purpose of sub-section (1) no person shall collect, store, process, disclose or otherwise handle any personal data of a natural person, intercept any communication of another person or carry out surveillance of another person except in accordance with the provisions of this Act.

Exemption- Nothing in this Act shall apply to —

1. the collection, storage, processing or dissemination of his own personal data by a natural person; or

- (2) surveillance by a resident of his own residential property, or
- (3) subject to obtaining the Privacy Commission's exemption under subsection (3) of section 16, the collection, storage or processing of anonymised data for non-commercial purposes or by any entity for academic, journalistic, research, statistical or archival purposes as required under the provisions of any other law for the time being in force.

Explanation.—For the purposes of this section, “non-commercial purposes” means permissible acts and omissions done in public interest which may be prescribed by the Privacy Commission through processes of public consultation with due regard to academics, civil society, experts and professional bodies.

chapter iii

protection of personal data

part a

notice by data controllers

Transparency in form and substance in all communications by Data Controllers-

1. All communications by data controllers shall be complied with in the following manner:
 - (a) in a concise, transparent, intelligible and easily accessible form, using clear and plain language, graphics and illustrations in particular for any information addressed specifically to a person below thirteen years of age;
 - (b) information shall be provided in writing, or by other means, including, where appropriate, by electronic means and when requested by the data subject, may be provided orally when deemed appropriate as per regulations that may be made by the Privacy Commission;
 - (c) requests for information by data subjects to data controllers shall be complied with promptly, ideally within a period of two working days noting acknowledgment of receipt and communicating the timelines for compliance that shall have a limit of one month from the date of receipt of the request for information:

Provided that all communications by the data controllers including but not limited to the rights of data subjects under this Part may be refused when the data controller may refuse to supply information to a data subject if he is unable to identify or has a well founded basis for reasonable doubt as to the identity of the data subject or are manifestly unfounded, excessive and repetitive, with respect to the information sought by the data subject;

Provided further that the data controller shall, while refusing to part away any information under foregoing provisions, provide reasons thereof;

(d) if the data controller refuses or fails to provide information, he shall specify reasons thereof along with remedies including appeal as provided under provisions of this Act.

(e) information shall include with a specific reference to the rights and remedies, include availability of measures for rectification, restriction and erasure as provided to data subjects under this Act.

2. The Privacy Commission, shall take special measures to ensure that information to be provided by the data controllers is accessible to all data subjects, including those who -

(a) are illiterate;

(b) suffer impaired or total lack of vision or hearing; and

(c) fall into any other category requiring special measures, as may be prescribed by the Privacy Commission:

Provided that, in case of any dispute, ambiguities in the terms of the notice and any privacy policies that apply shall be resolved in favour of the data subject.

3. The Privacy Commission may frame regulations to ensure compliance by data controllers of the rights to transparency and modalities of data subjects.

Part B

Consent of Data Subjects

Prior consent necessary to the collection of data –

1. Every Data Controller shall collect data from a data subject with his prior consent.

2. The consent of a data subject under sub-section (1) shall be deemed to have been validly effected only if it is —

(a) obtained from a person competent to contract in terms of section 11 of the Indian Contract Act, 1872;

(b) obtained in a free manner, in the terms of section 14 of the Indian Contract Act, 1872;

(c) informed and made with full knowledge of risks involved and the alternatives available;

(d) obtained prior to all data collection, except in the cases expressly excluded by section 12;

(e) voluntarily given through an express and affirmative Act and is recorded in modes including writing, audio, and visual media, which may be used in isolation or in conjunction;

Provided that effective consent shall be deemed to have been obtained where the written declaration of consent was given in a manner where it also concerned other matters, the request for consent shall be presented in a manner that is clearly distinguishable from the other matters in an intelligible and easily accessible form, using clear and plain language;

(f) a conspicuous means for its withdrawal is made available to the data subject; and

(g) withdrawn by the same means which were employed to obtain consent;

3. Obtaining consent of data subject for specific and limited as to purpose and duration,
4. Obtaining consent of data Subject for collection of data in a manner as prescribed by the Privacy Commission.

Explanation 1.— Consent shall be deemed to be limited only if it is obtained in respect of the purposes and duration strictly necessary to provide the product or service in relation to which personal data is sought to be collected, processed or disclosed.

Explanation 2.— When the purposes for which personal data was collected are materially altered or expanded subsequent to its collection, consent shall be deemed to be specific only if it is obtained afresh in respect of that alteration or expansion—

(a) after duly informing the data subject of the alteration or expansion in purpose; and

(b) prior to any use of that data for such expanded purposes; and

(c) in a manner as prescribed by the Privacy Commission

Special provisions in respect of data subjects lacking legal capacity to give consent

1. The consent in relation to personal data relating to data subject of unsound mind shall be effective only if it is obtained from a legal guardian, or such other person expressly empowered to act on behalf of such data subject under any law for the time being in force, or if it is in consonance with decision making capacity as laid down in section 4 of the Mental Healthcare Act, 2017:

Provided that where the unsoundness of mind is temporary, the data subject shall entitle to withdraw consent given on his behalf during the

period of such unsoundness of mind.

2. The consent in relation to personal data relating to data subjects of any other class of natural persons identified by the Privacy Commission shall be effective only if it satisfies all conditions set out in rules framed by the Privacy Commission.
3. All rights and entitlements conferred on data subjects under this Act shall be deemed to accrue to data subject as per consent on behalf of such persons.

Explanation. — Where no person acting on behalf of a data subject falling into any of the classes covered by this section can be identified despite the best efforts of the data controller or data processor, the State Privacy Commission, being accountable in a fiduciary capacity to the data subject, shall Act on behalf of such data subject.

Special provisions in respect to the processing of personal data of children.

1. The processing of personal data of a child by a data controller or data processor shall be lawful if it is in a manner that does not violate the stipulations prescribed in this section.
2. In respect of minors below the age of thirteen years, consent is to be obtained from a parent, legal guardian, or such other person acting in loco parentis as the case may be, after the minor is informed by the data controller in a simple and explanatory manner of the need for care in handling data concerning himself.
3. (3) Upon attaining age of majority, the data subject shall be entitled to:—
 - (a) be duly informed of the terms upon which personal data relating to his has been collected;
 - (b) alter or rescind the terms on consent; and 20
 - (c) require the destruction of all personal data relating to his.
4. The data controller or data processor shall make reasonable efforts, proportionate to the available technologies, to ensure that notice of the fiduciary's activities is served to the parent or legal guardian of a child of the processing of personal information of a child.
5. The notice under sub-section (4) shall be provided in the same manner for any material changes to processing priorly consented to.
6. The data controller or data processor shall make reasonable efforts, proportionate to the available technologies in obtaining verifiable parental consent.

7. The Data Fiduciary shall adopt appropriate methods for verifying parental consent on the basis of the following factors:—
 - (a) volume of personal data processed;
 - (b) proportion of such personal data likely to be that of children;
 - (c) possibility of harm to children arising out of processing of personal data; and
 - (d) such other factors as may be relevant.
8. The existing methods to obtain verifiable parental consent may include but not limited to—
 - (a) in making available a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, electronic scan or through other means available;
 - (b) permitting the use of a credit card/debit card/other online payment means with further verification through a confirmation call/other means to a parent/legal guardian/other for the purpose of a monetary transaction;
 - (c) obtaining consent through a parent confirmation call on a toll-free telephone number staffed by trained personnel;
 - (d) obtaining consent through a parent confirmation call to a trained personnel via video-conference:

Provided that, a data controller or data processor that does not disclose a child's personal information may use email or an inbuilt messaging function with additional steps to confirm that the person providing the consent is the parent;

Provided further that the information shall be provided to the parent so that consent may be revoked by using the same or other means in the future.
9. The data controllers or data processors shall ensure that there is no profiling, tracking, or behavioural monitoring of, or targeted advertising directed at children and undertaking any other processing of personal data that may cause significant harm to the child.

Special provisions in respect of data subjects unable to give consent.

1. The consent in relation to personal data relating to data subjects who are competent but temporarily unable due to any reason or circumstances to give consent shall be effective only if such consent is obtained in relation to purposes which are strictly necessary to uphold or advance the interests of the data subject or to the interests of the public, and the following conditions are fulfilled:—

- (a) in respect of data subjects who are declared missing under law and for the period they are missing, it is obtained from their nearest living relative, and where all reasonable means to contact their nearest living relative have been demonstrably exhausted, it is obtained from any person legally empowered to act on their behalf, or as a last resort, the appropriate State Privacy Commission in whose jurisdiction he was last resident;
- (b) in respect of data subjects who are detained, where all reasonable means to contact them, their nearest living relative have been demonstrably exhausted, it is obtained from any person legally empowered to act on their behalf, or as a last resort, the appropriate State Privacy Commission in whose jurisdiction he was last resident;
- (c) in respect of data subjects who are temporarily incapable for medical reasons and for the duration of their temporary incapacity, it shall be obtained from their nearest living relative, and where all reasonable means to contact their nearest living relative have been demonstrably exhausted or obtained from any person legally empowered to act in their behalf, or as a last resort, the appropriate State Privacy Commission in whose jurisdiction he was last resident:

Provided that when the inability to consent passes and where the personal data collected during the period of inability has not been anonymised, the data subject is entitled to—

- (i) alter or rescind the consent given on his behalf in all cases, and
- (ii) request the destruction of all records of personal data relating to him.

2. The consent in relation to personal data relating to data subjects who are unable, for reasons of death, and have not named a nominee to give, shall be effective only if it is obtained from -
 - (a) the nearest living relative; or
 - (b) where all reasonable measures to identify nearest living relative fail, the State Privacy Commission of the State in which the person last resided.

Collection of personal data. –

1. No person, including a data controller and data processor, shall collect any personal data without obtaining the consent of the data subject to whom it pertains.
2. Subject to sub-section (1), no person shall collect any personal data which is not necessary for the achievement of a purpose that is connected to a stated function of the person seeking its collection.

3. A person seeking to collect any personal data shall, prior to its collection and as prescribed by the Privacy Commission, inform the data subject without any direct or indirect charges, to whom such data pertains of the following details in respect of their personal data, namely —
 - (a) when it shall be collected;
 - (b) its content and nature;
 - (c) the purpose of its collection;
 - (d) the purpose and manner in which it shall be used;
 - (e) the persons to whom it shall be made available;
 - (f) the duration for which it shall be stored;
 - (g) the manner in which it may be accessed, checked and modified; 5
 - (h) the security practices and other safeguards, if any, to which it shall be subject;
 - (i) the privacy policies and other policies, if any, that shall protect it;
 - (j) whether, and the conditions and procedure upon which, it may be disclosed to others;
 - (k) the criteria, time and manner under which the personal data collected from the 10

data subject shall be destroyed;

 - (l) the time and manner under which the personal data collected from the data subject shall be destroyed on withdrawal of consent;
 - (m) the process, procedure and ability for a meaningful recourse in case of any grievance in relation to it; and 15
 - (n) the identity and contact details of the data controller and data processor.
4. The personal data collected in pursuance of a grant of consent by the data subject to whom it pertains shall, if that consent is subsequently withdrawn for any reason, be destroyed forthwith:

Provided that the person who collected the personal data in respect of which consent is subsequently withdrawn may, only if the personal data is necessary for the delivery of any good or the provision of any service, except where it is an essential service as provided under section 14, or the fulfillment of a lawful contract, not deliver that good or deny that service or fulfill that contract to the data subject who withdrew the grant of consent easily and at any point during the duration of a service.

Collection of personal data without prior consent. –

1. The data collector may collect or receive the personal data of a data subject from a third party without the prior consent of the data subject concerned only if it is—

(a) necessary for the provision of an emergency medical service or essential services as provided under section 14 to the data subject;

(b) strictly necessary to prevent, investigate or prosecute a cognizable offence as per process initiated, under the Code of Criminal Procedure, 1973 or by a law made through an Act of Parliament or State Legislature.

(c) exempted by the Privacy commission as per provisions relating to interception and surveillance under this Act:

Provided that for sub-sections (a) and (b) the data subject shall be duly informed in simple language and through a medium perfectly accessible to him, in a manner as prescribed by the Privacy Commission, at the earliest possible opportunity of the extent of personal data collected, and the processing and uses that it was put to in the course of meeting the purpose of the collection.

2. All personal data collected without prior consent under this section shall be destroyed as soon as the purpose for which it was collected is over :

Provided that where effective consent is obtained in terms and as per the safeguards under the Act at the earliest possible opportunity and not later than seven days from the date of the collection of the personal data, such personal data may continue to be stored and processed.

Special provisions in respect of data collected prior to the commencement of this Act. –

1. All data collected, processed and stored by data controllers and data processors prior to coming into force of this Act shall be destroyed within a period of two years from the date of coming into force of this Act.

2. Nothing in sub-section (1) shall apply where—

(a) consent in terms which satisfies all the requirements as provided for under this Act and is obtained afresh within the aforementioned period of two years; or

(b) The personal data collected prior to the commencement of this Act was anonymised in such a manner as to make re-identification of the data subject absolutely impossible.

Explanation.—For the purpose of this section 'consent' shall be deemed to have been obtained if the data subject does not explicitly withdraw

consent, on the basis of a specific notification in this regard, issued by data controller to the data subject, in a manner as prescribed by the Privacy Commission, within the aforementioned period of two years.

Part C

Further limitations on Data Controllers

. Bar on denial of subsidies, benefits and entitlements.

1. No essential services, shall be withheld on the ground that consent to share personal data in a particular manner for the purpose of identification, has not been obtained or has been withheld or such data has not been collected at the time the data subject claims the service:

Provided that the data subject shall be entitled to damages where an essential service has been denied:

Provided further that the data controller or data processor shall accept any alternate means for identification, wherever available as per the choice of the data subject:

Provided also that the data subject shall be entitled to exemplary damages where an essential service has been denied despite the existence of pre-existing alternative means of identifying the data subject.

2. An essential service includes the following, namely:—

- (a) subsidies, benefits and entitlements which are provided on establishing the identity of an individual under the Aadhaar Act, 2016;
- (b) entitlements under the Public Distribution System including but not limited to the provisions under the National Food Security Act, 2013;
- (c) the provision of medical care to minors, expectant mothers or those requiring emergent or life-saving care;
- (d) social security benefits, including pension, gratuity and provident fund;
- (e) benefits under the Mahatma Gandhi National Rural Employment Guarantee Act, 2005;
- (f) services provided to effectuate the provisions of Part III or Part IV of the Constitution;
- (g) any other service additionally prescribed by the appropriate Government by notification in the Official Gazette or by way of a public proclamation;

3. Where an essential service is provided under sub-section (1) and the provider of the said service can demonstrate grave and irreparable injury arising directly from the unavailability of personal data in respect of which

consent was sought, it may approach the Privacy Commission for relief or seeking exemption.

Storage and destruction of personal data. –

1. No person shall store any personal data for a period longer than is necessary to achieve the purpose for which it was collected or received, or, if that purpose is achieved or ceases to exist for any reason, for any period following such achievement or cessation.
2. Save as provided in sub-section (3), any personal data collected or received in relation to the achievement of a purpose shall, if that purpose is achieved or ceases to exist for any reason, be destroyed forthwith.

Provided that where the purpose of collection is the provision of essential services under Section 14 or of banking as provided under Section 5(b) of the Banking Regulation Act, 1949, the data subject shall be duly informed in terms to be prescribed by the Privacy Commission of the impending destruction of the data.

3. Notwithstanding anything contained in this section, any personal data may be stored for a period longer than is necessary to achieve the purpose for which it was collected or received, or, if that purpose has been achieved or ceases to exist for any reason, for any period following such achievement or cessation, if—
 - (a) the data subject to whom it pertains grants their effective consent to such storage prior to the purpose for which it was collected or received being achieved or ceased to exist;
 - (b) it is adduced for an evidentiary purpose in a legal proceeding; or
 - (c) it is required to be stored for historical, statistical or research purposes under the provisions of an Act of Parliament and specified in a manner as prescribed by the Privacy Commission:

Provided that only such amount of personal data that is necessary to achieve the purpose of storage under this sub-section shall be stored and any personal data that is not required to be stored for such purpose shall be destroyed forthwith:

Provided further that any personal data stored under this sub-section shall, to the extent possible, be anonymised.

Processing of personal data. –

1. Save as provided in sub-section (2), no person shall process any personal data that is not necessary for the achievement of the purpose for which it was collected or received.

2. Notwithstanding anything contained in this section, any personal data may be processed for a purpose other than the purpose for which it was collected or received only if —
 - (a) the data subject grants his effective consent to the processing and only that amount of personal data that is necessary to achieve such other purpose is processed;
 - (b) it is necessary to perform a contractual duty to the data subject;
 - (c) it is necessary to prevent an imminent threat to the security of the State or public order and the fact of such threat is recorded in writing by a competent organization which anticipates such a threat; or
 - (d) it is necessary to prevent, investigate or prosecute a cognizable offence.
3. Notwithstanding anything contained in this section personal data may be anonymized, as a measure to enhance the security of the data and the privacy of the data subject:

Provided that anonymized data may be processed or disseminated only if the data controller has ensured the Privacy Commission that it is impossible to identify the data subject to whom it relates and sought exemption:

Provided further that where the Privacy Commission is satisfied that the personal data has been satisfactorily anonymized, the Privacy Commission may grant an extension on the permissible period of storage and disclosures for specified purposes in addition to those in respect of which effective consent was obtained.

Security of personal data and duty of confidentiality-

1. No person shall collect, receive, store, process or otherwise handle any personal data without implementing measures, including, but not restricted to, technological, physical and administrative measures, adequate to secure its confidentiality, secrecy, integrity and safety, including from theft, loss, damage or destruction.
2. Any person who collects, receives, stores, processes or otherwise handles any personal data shall maintain confidentiality and secrecy in respect of data collected, received, stored, processed or in their possession.
3. It shall be the duty of the data controllers and data processors to maintain confidentiality and secrecy in respect of personal data in their possession or control.
4. Without prejudice to the generality of the foregoing provisions of this section and notwithstanding any law for the time being in force, any person who collects, receives, stores, processes or otherwise handles any personal data shall, if its confidentiality, secrecy, integrity or safety is

violated by theft, loss, negligence, damage or destruction, or as a result of any collection, processing or disclosure contrary to the provisions of this Act, or for any other reason whatsoever, as soon as he becomes aware of such violation, notify the person to whom it pertains, the Privacy Commission and any other agencies as may be designated for the purpose by the Central Government in such form and manner as may be prescribed.

5. Any person, who collects, receives, stores, processes, or otherwise handles any personal data shall report all violations of provisions of this Chapter to the Privacy Commission, that are brought to its notice, or are reasonably expected to be known to such persons.

Transfer of personal data outside the territory of India.

1. Subject to the provisions of this section, personal data that has been collected according to this Act may be transferred by a data controller to a data processor located in India, if the transfer is pursuant to an agreement that demonstrably and expressly binds the data processor to same or stronger conditions and measures in respect of the storage, processing, destruction, disclosure and other handling of the personal data as are contained in this Act.
2. No data controller shall transfer personal data outside the territory of India or to an international organisation unless any one of the following conditions is fulfilled—
 - (a) the Central Government has issued a notification indicating it has decided that the country, territory, or international organization in question agrees to ensure an adequate level of protection of privacy and personal data in a manner which is in no way incompatible with the privacy principles contained in section 3:

Provided that any such notification of an adequacy decision shall only be issued by the Central Government after due consultation with the Privacy Commission and its Office of data protection, and after having taken inputs from such stakeholders and experts as the later may recommend; or
 - (b) The transfer by the data controller to a data processor located outside India is pursuant to an agreement that binds the recipient of the personal data to the strict conditions and measures in respect of the storage, processing, destruction, disclosure, and other handling of the personal data as contained in this Act; or
 - (c) The data controller shall assess all the circumstances relating to transfer of personal data in question to the third country, territory, or international organization and concluded that appropriate legal instruments and safeguards exist to protect the data, and inform the Office of data protection of the Privacy Commission of such transfers of data:

Provided that while informing the transfer of personal data to the Privacy Commission, the data controller shall maintain following details, namely:—

- (i) the date and time of the transfer;
- (ii) the name of other pertinent information about the data processor;
- (iii) the justification for the transfer;
- (iv) a description of the personal data transferred; and
- (v) the existing legal instruments and safeguards for data protection by which the data processor is bound.

3. No data processor shall process any personal data transferred under this section except to achieve the purpose for which it was collected.
4. Any data controller who transfers personal data under this section shall be responsible to the data subject for the actions of the data processor.
5. Any data controller who transfers personal data outside the territory of India shall comply with the provisions of this Act notwithstanding the fact that the personal data in question is being processed outside the country.

Explanation.—For the purpose of this section, the duties of a data collector shall include, but not be limited to:

- (a) ensure that any recipient of such transferred personal data takes appropriate steps to ensure compliance with the provisions of this Act;
- (b) report any breach to the Privacy Commission notwithstanding the transfer of such data outside the territory of India.

Disclosure of personal data –

1. Save as provided in this Chapter, no person including the Data Controller shall disclose, or otherwise cause any other person to receive, the content or nature of any personal data, including any other details in respect thereof, except to the person to whom it pertains.
2. No person including the Data Controller shall disclose any personal data without obtaining the prior effective consent of the data subject:

Provided that consent of a data subject obtained by way of threat, under duress or coercion or denial of service shall not be treated as a valid and effective consent.

3. For the purpose of sub-section (2), a person including the data controller seeking to disclose any personal data shall, prior to its disclosure, inform

the data subject of the following details in respect of their personal data, namely: —

- (a) when and to whom it shall be disclosed;
 - (b) the purpose of its disclosure;
 - (c) the security practices and other safeguards, if any, to which personal data shall be subject to;
 - (d) the privacy policies and other policies, if any, that shall protect personal data;
 - (e) the procedure for recourse in case of any grievance in relation to personal data; and
 - (f) any other details prescribed by rules or by the Privacy Commission.
4. (4) Notwithstanding anything contained in this section, any person who collects, receives, stores, processes or otherwise handles any personal data may disclose it to a 35 person other than the data subject, whether located in India or otherwise, for the purpose of only processing it to achieve the purpose for which it was collected:
- Provided that in case disclosure is pursuant to an agreement that explicitly binds the person receiving it to same or stronger measures in respect of its storage, processing, destruction, disclosure or other handling as are contained in this Act.
5. Any disclosure of personal data made contrary to the provisions of this Act shall be notified to the Data Subject and Privacy Commission.

Special provisions for sensitive personal data –

1. Notwithstanding anything contained in this Act and any other law for the time being in force —
 - (a) no person shall collect sensitive personal data without effective consent from the data subject;
 - (b) no person shall store sensitive personal data for a period longer than is strictly necessary to the purpose for which it was collected or received, or, if that purpose has been achieved or ceases to exist for any reason, for any period following such achievement or cessation;
 - (c) no person shall process sensitive personal data for any purpose other than the purpose for which it was collected or received;
 - (d) no person shall disclose sensitive personal data to another person, or otherwise cause any other person to come into the knowledge or possession

of, the content or nature of any sensitive personal data, including any other details in respect thereof, except the data subject.

2. In addition to the requirements set out under sub-clause (1), the Privacy Commission shall set out additional protections in respect of:—
 - (a) sensitive personal data relating to data subjects who are minors;
 - (b) biometric and deoxyribonucleic acid data; and
 - (c) financial and credit data.

Special provisions for data impact assessment-

1. Where the data controller uses, directly or indirectly any new technology, it shall be the duty of data controller to assess the risks involved in using new technology to the data protection rights under this Act.
2. The data controller shall conduct an internal process of a data protection impact assessment which shall include a systematic and extensive evaluation of the personal aspects relating to data subjects especially the impact on their legal and human rights which result from use of the new technology.
3. The assessment shall include—
 - (a) a systematic description of the processing operations and the purposes for such processing;
 - (b) an assessment of compliance with the principles of protecting privacy in relation to the purposes;
 - (c) an assessment of the impact on the risks to the rights and freedoms of data subjects; and
 - (d) the safeguards, security measures and mechanisms to address risks to protection of personal data.
4. All data impact assessment reports will be submitted periodically to the State Privacy commission as per the rules and regulations made under this Act.
5. The State Privacy Commission shall prepare and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment.
6. The lists prepared under sub-section(4) shall be communicated to the Office for Data Protection of the Privacy Commission for approval prior to adoption.

Explanation.—The term “new technology” includes any pre-existing technology used for a new purpose through an iterative process by which any existing or pre-existing process or output is substantially changed.

Part D

Rights of a data subject

Right to access for data subject

1. The data subject shall have the right to obtain from the data controller information as to whether any personal data concerning him is collected or processed, and, where any such personal data has been collected or processed by the data controller, access to the personal data shall be granted along with the following information—
 - (a) the purposes of the storage and processing personal data;
 - (b) the categories of the personal data concerned;
 - (c) the recipients or categories of recipients to whom the personal data have been or shall be disclosed, in particular to determine that period;
 - (d) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data 5 subject or to object to such processing;
 - (e) the right to lodge a complaint with a supervisory authority;
 - (f) where the personal data are not collected from the data subject, any available information as to their source;
 - (g) the existence of automated decision making, including profiling.
2. When the personal data is transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the safeguards as per provisions of this Act
3. The data controller shall provide a single copy of the personal data undergoing processing to the data subject and additional copies may be subject to additional charges on a concessional and reasonable basis
4. The right to access data by a data subject shall be in addition to the notifications and existing obligations of data controllers not limited to, but including the right to seek information of security breaches to their personal data.

Right to rectification for Data Subjects and obligations of Data Controllers.

1. The data subject shall have the right to obtain from the data controller promptly the rectification of inaccurate information in his personal data.
2. Any Data Controller who collects, receives, stores, processes or otherwise handles any personal data shall, to the extent possible, ensure that it is accurate and, where necessary, is kept up to date.
3. No data controller who collects, receives, stores, processes or otherwise handles any personal data shall deny, to the data subject, the opportunity to review and obtain a copy of such data and, where necessary, rectify anything that is inaccurate or not up to date.
4. The data controller shall issue special notice to the data subject of any rectification of personal data pertaining to the data subject unless such a move proves impossible or involves disproportionate effort

Right to destruction of personal data-

1. The data subject shall have a right to request destruction of data at any time, and data controllers and processors shall comply with such requests, within a timeframe, manner and mode to be prescribed by the Privacy Commission.
2. The data subject shall have the right to obtain from the data controller the erasure of his personal data without any delay and the Data Controller shall have duty to erase personal data without undue delay where one of the following grounds are applicable:
 - (a) the personal data is no longer necessary in relation to the purposes for which it was collected or processed and causes actual harm;
 - (b) the data subject withdraws consent as per the provisions of this Act and no other legal ground for processing continues to exist;
 - (c) the personal data has been unlawfully processed.
3. The provisions of this section shall not apply when the storage or processing is determined by the Privacy Commission to be:
 - (a) for exercising the right of speech and freedom of expression which includes the right to receive information, especially about public personalities, officials or matters of public interest.
 - (b) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and the erasure is likely to be or render impossible or seriously impair such objectives.

- (c) for the establishment, exercise or defense of any legal proceedings.
 - (d) as per the provisions of this Act including but not limited to anonymised data as contained under section 16.
4. The data controller shall issue special notice to the data subject of any destruction of his personal data unless such a move proves impossible or involves disproportionate effort.

Right to restriction of processing-

1. The data subject shall have the right to obtain from the data controller restriction of processing of personal data where one of the following applies—
 - (a) the accuracy of the personal data is contested by the data subject, for a period enabling the data controller to verify the accuracy of the personal data;
 - (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of its use instead;
 - (c) the data controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense in legal proceedings;
 - (d) the data subject has objected to processing pending verification whether the legitimate grounds of the data controller override those of the data subject.
2. When the processing has been restricted under this provision, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defense in legal proceedings or for the protection of the rights of another natural person.
3. A data subject who has obtained restriction of processing pursuant to this section shall be informed by the data controller before the restriction of processing is removed.

Right to object

1. The Data Subject shall have the right to object, on grounds relating to her particular situation, at any time to processing of personal data concerning her which is based on the principles for protection of privacy as provided under Section 3 of the Act.
2. The Data Controller shall in addition to its other obligations, for communication of notices to the Data Subject under this act shall at

the latest at the time of the first communication with the Data Subject provide notice to the Data Subject of its right to object, clearly and separately from other information.

Right to portability of personal data –

1. The data subject shall have the right to receive all personal data concerning him from any data controller within a reasonable time and in a structured, commonly used and machine-readable format upon request.
2. Except where it is expressly precluded by any law for the time being in force, the data subject shall have the additional right to receive the output of all processing of his personal data within a reasonable time.
3. The data controller shall not hinder in any manner the transfer by the data subject, of the personal data, to any other person.
4. The data subject shall have the right to request that the personal data be transmitted directly from one controller to another, in all instances where it is technically feasible, and the data subject be informed upon the completion of the such transmission:
Provided that no transmission shall be deemed to be complete until all records of the data so transmitted as per the instructions of the data subject are then destroyed by the data controller to whom request is made.
5. Where the data controller claims that it is not technically feasible to transfer data in the manner provided for under sub-section (4) and the data subject challenges such a claim in terms of rules prescribed by the Privacy Commission in this regard, the burden to prove a lack of technical feasibility to transfer falls upon the data controller.

Right to seek exemption from automated decision-making –

1. The data subject in addition to other rights with respect to processing of personal data shall specifically have the right to seek exemption from decisions based solely on automated processing including profiling, which produces legal effects concerning or significantly affecting including but not limited to when it causes demonstrable harm or injury.
2. The provisions of sub-section (1) shall not apply, if the automated decision:—
 - (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

- (b) is based on the data subject's express and explicit consent;
- (c) is provided a case by case exemption in cases by the Privacy Commission having regard to the principles as provided under section 3.

Explanation.— The term “case by case exemption” applies to an individual person but does not include a category or a class of personal data.

3. The data controller shall provide additional safeguards with specific provisions for the right of the data subject on the part of the Data controller for providing an effective process of hearing and contesting decisions.
4. All decisions made by way of automated decision by data controllers shall be open to legal remedies including appeals as provided under this Act.

chapter IV

INTERCEPTION AND SURVEILLANCE

Special provisions for competent organizations.

1. All provisions of Chapter III shall apply to personal data collected, processed, stored, transferred or disclosed by competent organizations unless specifically provided or exempted under this Chapter;
- (2) A competent organization seeking to exclude the application of provisions of Chapter III with respect to all categories of personal data collected, processed, stored, transferred or disclosed by itself, shall prefer an application with the Privacy Commission, in a manner prescribed by the Privacy Commission.
 - (3) An application under sub-section (2) shall specify—
 - (a) the specific personal data sought to be exempted from provisions of Chapter III of this Act;
 - (b) the reasons as to why surveillance under this provision is necessary to prevent a reasonable threat to security of the State or public order :
Provided that the reasons shall also state why the data covered under the request for exemption has a reasonable, proximity and direct nexus with the threat:
 - Provided further that the reasons shall specify why a lesser restrictive measure may not be taken; and
 - (c) the specific time period during which the exemption is sought.
 - (4) No competent organisation shall process or store any personal data without implementing measures to ensure that the number of persons

within that intelligence organisation to whom it is made available, and the extent to which it is copied, is limited to the minimum that is necessary to fulfill the purpose for which it is processed or stored, as the case may be.

(5) Notwithstanding any provisions of the Indian Evidence Act, 1872 any personal data collected, processed, stored, transferred or disclosed by a competent organization in contravention of this Act shall be inadmissible in legal proceedings before any court of law.

Bar against interception of communications.

1. Notwithstanding anything contained in any other law for the time being in force, but save as provided in this chapter, no person shall intercept, or cause to be intercepted, any communication of another person person except in pursuance of an order by the appropriate Surveillance and Interception Review Division.
2. No interception of any communication shall be ordered or carried out that is not necessary to achieve the purpose for which the interception is sought.

Prior authorisation by the appropriate Surveillance and Interception Review Division –

1. An authorised officer of a competent organisation seeking to intercept any communication of another person shall prefer an application, in such form and manner as may be prescribed by the Central Government in consultation with the Privacy Commission, to the appropriate Surveillance and Interception Review Division.
2. The appropriate Surveillance and Interception Review Division may, if it is satisfied that the interception is necessary to prevent a reasonable threat to security of the State or public order, or prevent, investigate or prosecute a cognisable offence, order the interception of communications by recording reasons in writing.
3. The appropriate Surveillance and Interception Review Division shall, prior to issuing an order for interception of any communication, satisfy itself that all other lawful means to acquire the information sought to be intercepted have been exhausted and that the proposed interception is necessary and proportionate, reasonable and not excessive.
4. Any interception of any communication ordered, authorised or carried out prior to the commencement of this Act shall, immediately upon the

constitution of the Privacy Commission, be reported to the Office for Surveillance Reform of the Privacy Commission.

5. Any interception involving the infringement of the privacy of individuals who are not the subject of the intended interception, or where communications relate to journalistic, activism related to fundamental and constitutional rights, parliamentary or legally privileged material is involved, it shall satisfy additional conditions including the provision of specific prior justification in writing to the Office for Surveillance Reform of the Privacy Commission as to the necessity for the interception and the safeguards providing for minimizing the material intercepted to the greatest extent possible and the destruction of all such material that is not strictly necessary for the purpose of the interception.

Authorisation by Home Secretary in emergent circumstances –

1. Notwithstanding anything contained in section 31, if the Home Secretary of the appropriate Government is satisfied that an imminent grave threat to the security of the State or public order exists, he may, for reasons to be recorded in writing, order the interception of any communication.
2. No order for interception of any communication made under this section shall be valid upon the expiry of a period of seven days from the date of the order.
3. Before the expiry of a period of seven days under this section, the person who carried out the interception of communication shall notify the appropriate Surveillance and Interception Review Division of the fact of such interception, the name and address of the person whose communication is being intercepted, and the duration of the interception and, furthermore, shall furnish a copy of the order of the Home Secretary authorising the interception.
4. The surveillance and Interception Review Division may, upon receipt of notification under sub-section (3), recall the order on grounds of lack of an imminent and grave threat to the security of State or public order, or on absence of ground mentioned in sub-section (2) of section 31, and may also order for damages in case of abuse to be paid to the individual/ natural person whose communication was intercepted under the order so recalled.

Duration of interception –

1. An order for interception of any communication shall specify the period of its validity and upon the expiry of the period of validity of all interception

carried out in relation to that order shall cease forthwith:

Provided that no order for interception of any communication shall be valid upon the expiry of a period of thirty days from the date of the order.

2. The appropriate Surveillance and Interception Review Division, may, upon receipt of an application from an authorised officer in such form and manner as may be prescribed by the Central Government in consultation with the Privacy Commission, renew, for a period not exceeding thirty days, any order for interception of any communication if it is satisfied that the conditions upon which the original order was issued continue to exist:

Provided that where interception of communication, under orders passed under this Chapter, including orders for renewal, has been carried out for a cumulative period of six months, whether in succession or not, any application for further renewal, shall be accepted, if in addition to the ground mentioned in this sub-section, the competent organization is able to demonstrate the need for such continued interception.

Duty to inform the person concerned –

1. Subject to sub-section (2), before the expiry of a period of thirty days from the conclusion of any interception of communication ordered or carried out under this Act or any interception of communication carried out before the Act came into force, the authorised officer who carried out the interception of communication shall, in writing in such form and manner as may be prescribed by the Central Government in consultation with the Privacy Commission, notify, with reference to the relevant order of the Surveillance and Interception Review Division, each person whose communication was intercepted of the fact of such interception and duration thereof.
2. The Surveillance and Interception Review Division may, on an application made by an authorised officer in such form and manner as may be prescribed, if he is satisfied that the person(s) specified in notification under sub-section (1) poses a reasonable threat to the security of the State or public order or adversely affect the prevention, investigation or prosecution of a cognisable offence, for reasons to be recorded in writing addressed to the authorised officer, order that such person(s) whose communication was intercepted not be notified of the fact of such interception or the duration thereof:

Provided that any order passed preventing disclosure of interception under section (2) shall not operate in infinity and shall record reasons in writing with the period till when the reasonable threat is anticipated to extend, on cessation of which the duty to inform under sub-section (1) shall operate.

Security and duty of data security and privacy –

1. Any person who carries out any interception of any communication, or who obtains any information, including personal data, as a result of an interception of communication, shall have a duty of data security and privacy with respect to it.
2. No person shall intercept any communication of another person without implementing measures, including, but not restricted to, technological, physical and administrative measures, to secure the data security and privacy of all information obtained as a result of an interception of communication, including from theft, negligence, loss or unauthorised disclosure.
3. Every competent organisation shall, before the expiry of a period of one hundred days from the enactment of this Act, designate as many officers as it deems fit as Privacy Officers who shall be administratively responsible for ensuring that all interceptions of communications carried out by that competent organisation are in compliance with the provisions of this Chapter.

Disclosure of intercepted communications –

1. In addition to the existing obligations and duties for lawful interception, no person shall disclose to any person, other than the person whose communication has been intercepted, or otherwise cause any other person to come into the knowledge or possession of, the content or nature of any information, including personal data, obtained as a result of an interception of any communication including the fact that the interception of communication was carried out.
2. Notwithstanding anything contained in this section, if the disclosure of any information, including personal data, obtained as a result of an interception of any communication is necessary to prevent a reasonable threat to the security of the State or public order, or prevent, investigate or prosecute a cognisable offence, an authorised officer may disclose the information, including personal data, obtained as a result of the interception of any communication to any authorised officer of any other competent organization:

Provided that no authorised officer shall disclose any information, including personal data, obtained as a result of the interception of any communication that is not necessary to achieve the purpose for which the disclosure is sought.

Storage and destruction of intercepted communications –

1. Subject to sub-section (2), no person shall store any data, including personal data, obtained as a result of an interception of any communication for a period longer than one hundred and eighty days from the date on which the last order for interception of the communication to which the obtained information pertains expired and upon expiry of such period, shall destroy the data so stored.
2. The Surveillance and Interception Review Division may, on an application made in such form and manner as may be prescribed by the Privacy Commission, if it is satisfied that it is necessary to—
 - (a) prevent a reasonable threat to the security of the State; or
 - (b) maintain public order; or
 - (c) prevent, investigate or prosecute a cognisable offence in an ongoing legal proceeding and is authorized by a court order to that effect;for reasons to be recorded in writing, order that any information, including personal data, obtained as a result of an interception of any communication may be stored for a period longer than one hundred and eighty days from the date on which the last order for interception of the communication to which the obtained information pertains expired and shall not be destroyed.
3. Any data obtained as a result of interception of any communication shall be stored in a manner that complies with the provisions of Section 15 with respect to such data.

Bar against surveillance-

1. Notwithstanding anything contained in any other law for the time being in force, but save as provided in this chapter, no person shall order or carry out, or cause or assist the ordering or carrying out of, any surveillance of another person.
2. The appropriate Surveillance and Interception Review Division shall have the power to issue appropriate directions, including for cessation of any activity, being carried out by a person, including a statutory authority, which is in contravention of the proviso to sub-section (1).

Surveillance by the State –

1. No member of a competent organization shall order or carry out, or cause to be ordered or carried out, any surveillance of another person save in pursuance of an order by the appropriate Surveillance and Interception Review Division.
2. No surveillance shall be ordered or carried out that is not necessary to achieve the purpose for which the surveillance is sought.

3. An authorised officer seeking to carry out any surveillance of another person shall prefer an application, in such form and manner as may be prescribed by Central Government in consultation with the Privacy Commission, to the Surveillance and Interception Review Division.
4. The Surveillance and Interception Review Division may, if it is satisfied that the surveillance is necessary to prevent a reasonable threat to the security of the State or public order, or to prevent, investigate or prosecute a cognisable offence, for reasons to be recorded in writing addressed to the authorised officer, order the surveillance.

Surveillance by private persons or entities –

1. Notwithstanding anything contained in any other law for the time being in force, and without prejudice to the provisions of section 37 of this Act, no person who is not a member of a competent organization shall carry out, or cause to be carried out, any surveillance in any public place or in any property or premises that is not in his possession.
2. Without prejudice to sub-section (1), any person who carries out any surveillance under this section shall be subject to a duty to inform, in such manner as may be prescribed by the Central Government in consultation with the Privacy Commission, members of the public of such surveillance.

Duration of surveillance –

1. An order for surveillance shall specify the period of its validity and, upon the expiry of the validity of the order, all surveillance carried out in relation to that order shall cease forthwith:

Provided that no order for surveillance shall be valid upon the expiry of a period of thirty days from the date of the order.

2. The Surveillance and Interception Review Division may, upon receipt of an application from an authorised officer in such form and manner as may be prescribed by the Central Government in consultation with the Privacy Commission, renew any order for surveillance if it is satisfied that the conditions upon which the original order was issued continue to exist.

Provided that where surveillance, under orders passed under this Chapter, including orders for renewal, has been carried out for a cumulative period of six months, whether in succession or not, any application for further renewal, shall be accepted, if in addition to the ground mentioned in this

sub-section, the competent organization is able to demonstrate the need for such continued surveillance.

Duty to inform the person concerned –

1. Subject to sub-section (2), before the expiry of a period of thirty days from the conclusion of any surveillance ordered or carried out under this Act or any surveillance carried out before this Act came into operation, the authorised officer who carried out the surveillance shall, in writing in such form and manner as may be prescribed by the Central Government in consultation with the Privacy Commission, notify, with reference to the relevant order of the Surveillance and Interception Review Division, each person in respect of whom surveillance was carried out of the fact of such surveillance and duration thereof.
2. The appropriate Surveillance and Interception Review Division may, on an application made by an authorised officer in such form and manner as may be prescribed by the Central Government in consultation with the Privacy Commission, if it is satisfied that the notification under sub-section (1) would present a reasonable threat to the security of the state or public order, or adversely affect the prevention, investigation or prosecution of a cognisable offence, for reasons to be recorded in writing addressed to the authorised officer, order that the person not be notified of the fact of such surveillance or the duration thereof:

Provided any order passed preventing disclosure of surveillance under Section (2) shall not operate indefinitely and shall record reasons in writing with the period till when the reasonable threat is anticipated to extend, on cessation of which the duty to inform under sub-section (1) shall operate.

Security and duty of confidentiality and secrecy –

1. Any person who carries out any surveillance, or who lawfully obtains any information, including personal data, as a result of surveillance, shall be subject to a duty of confidentiality and secrecy in respect of it.
2. No person shall carry out any surveillance of another person without implementing measures, including, but not restricted to, technological, physical and administrative measures, to secure the confidentiality and secrecy of all information obtained as a result of surveillance, including from theft, loss or unauthorised disclosure.
3. Every competent organization shall, before the expiry of a period of one hundred days from the enactment of this Act, designate as many officers as it deems fit as Privacy Officers who shall be administratively

responsible for ensuring that all surveillance carried out by the Competent Organization are in compliance with the provisions of this Chapter:

Provided that a public authority that does not order or carry out surveillance shall not be required to designate any Privacy Officers under this sub-section.

4. Every person who is not a member of a competent organization and who seeks to carry out any surveillance shall, at least seven days before the surveillance is first carried out, designate or appoint as many persons as it deems fit as Privacy Officers who shall be responsible for ensuring that all surveillance carried out is in compliance with the provisions of this Chapter:

Provided that where surveillance is carried out by a single person, that person shall be deemed to be a Privacy Officer.

Disclosure of surveillance –

1. In addition to the existing obligations and duties for lawful, no person shall disclose to any person, other than the person who is being surveilled, or otherwise cause any other person to come into the knowledge or possession of, the content or nature of any information, including personal data, obtained as a result of any surveillance including the fact that the surveillance was carried out.
2. Notwithstanding anything contained in this section, if the disclosure of any information, including personal data, obtained as a result of surveillance is necessary to prevent a reasonable threat to the security of the State or public order, or prevent, investigate or prosecute a cognisable offence, that information, including personal data, obtained as a result of surveillance may be disclosed to an authorized officer of a competent organization only:

Provided that no person shall disclose any information, including personal data, obtained as a result of surveillance that is not necessary to achieve the purpose for which the disclosure is sought.

Storage and destruction of surveillance

1. Subject to sub-section (2), no person shall store any information, including personal data, obtained as a result of surveillance for a period longer than one hundred and eighty days from the date on which the surveillance to which the obtained information pertains ceased, and upon expiry of such period, shall destroy the data so stored.

2. The appropriate Surveillance and Interception Review Division may, on an application made in such form and manner as may be prescribed by the Central Government in consultation with the Privacy Commission, if it is satisfied that it is necessary to—
 - (a) prevent a reasonable threat to the security of the State; or
 - (b) public order; or
 - (c) prevent, investigate or prosecute a cognisable offence in an ongoing legal proceeding and is authorized by a court order to that effect;for reasons to be recorded in writing, order that any information, including personal data, obtained as a result of surveillance may be stored for a period longer than one hundred and eighty days from the date on which the last order for surveillance to which the obtained information pertains expired and shall not be destroyed.
3. Any data obtained as a result of surveillance shall be stored in a manner that complies with the provisions of Section 14 with respect to such data.

Exception regarding reporting of violation of provisions of this Act -

1. Any communication, complaint, or evidence thereunder alleging violation of the provisions of this Act or other applicable law, if made to the Privacy Commission, the Surveillance and Interception Review Divisions and their legal counsel, or to the Supreme Court, shall not be treated as a violation of this Act and applicable provisions of the Information Technology Act, 2000.

CHAPTER V

The Privacy Commission

Constitution of the Privacy Commission

1. The Central Government shall, by notification, issued within 6 months of the enactment of this Act, constitute, with immediate effect, a body to be called the Privacy Commission, by warrant under its hand and seal, to exercise the jurisdiction and powers and discharge the functions and duties conferred or imposed upon it by or under this Act.
2. The Privacy Commission shall be composed of at least three Privacy Commissioners, to be appointed by the President as specified by this Act.
3. The Privacy Commission shall consist of two coordinate offices, namely the Office for Data Protection and the Office for Surveillance and Interception Reform, and such officers, other employees, and experts as may be appointed in accordance with the provisions of this Act.

4. The Privacy Commission shall be autonomous, independent, and free from external interference. It shall be provided with sufficient operational resources including human, technical, and financial for the effective discharge of its duties and exercise of its powers. Such powers shall be subject to audit by the Comptroller and Auditor General of India.
5. The exercise of financial powers shall be subject to audit by the Comptroller and Auditor General of India.

Appointment and Qualifications of Privacy Commissioners of Privacy Commission

1. The Privacy Commission shall consist of one Chief Privacy Commissioner and two or more than two Privacy Commissioners as may be deemed necessary:

Provided that at least one Privacy Commissioner shall be a person who has been a Judge of the Supreme Court or has been a Chief Justice or Acting Chief Justice of a High Court:

Provided further that at least one or more Privacy Commissioner shall be a woman or a member of the third gender, or a transgender:

Provided also that at least one or more Privacy Commissioner shall belong to a —

- (i) socially or educationally backward classes; or
- (ii) Scheduled Caste; or
- (iii) Scheduled Tribe; or
- (iv) minority.

(2) The Chief Privacy Commissioner and the Privacy Commissioners shall be persons of outstanding ability, impeccable integrity and standing and who have special knowledge of, technical expertise in, and professional or academic experience, of not less than ten years cumulatively, in any one or more of the following domains—

- (a) privacy law and policy;
- (b) business and human rights;
- (c) civil liberties;
- (d) engineering, technology, design and ethics; or
- (e) data collection, storage and protection practices, including emerging technologies.

(3) The Central Government shall issue a public advertisement inviting applications to fill all vacancies in the Privacy Commission.

(4) The selection committee for the appointment of the members of the Privacy Commission, shall be constituted by the President of India and the selection panel shall consist of the following, namely :—

- (a) collegium of the Supreme Court of India;
- (b) the Law Minister;
- (c) the Leader of the Opposition in Lok Sabha or of the single largest opposition party being one with the greatest numerical strength in the Lok Sabha;
- (d) Director of Indian Institute of Science;
- (e) Director of an Indian Institute of Technology as appointed by the IIT Council;
- (f) one eminent person representing the private sector; and
- (g) one eminent person representing the civil society.

Explanation.—The term 'civil society' mean non-Governmental and non-profit organisations that engage in the general upliftment and interests of the people in the field of privacy and is independent of Government funding, interference or influence.

(5) All proceedings of the selection committee shall be matters of public record and subject to pro-active disclosures under the Right to Information Act, 2005.

(6) No Members of Parliament or Members of the Legislature of any State or Union territory having Legislative Assembly or a member of any political party shall be eligible for

selection or appointment as a Chief Privacy Commissioner or Privacy Commissioner:

Provided that persons holding any other office of profit or carrying on any business or practising any profession, before he enters upon this office, shall be eligible for appointment or selection as Chief Privacy Commissioner or Privacy Commissioner, as the case may be, if—

- (a) he holds any office of trust or profit, resigns from such office; or
- (b) he is carrying on any business, severs his connection with the conduct and management of such business; or
- (c) she is practising any profession, ceases to practise such profession.

Composition of the Office for Data Protection of the Privacy Commission

1. The office for Data Protection of the Privacy Commission shall be consisted of a Director General of Data Protection, to be appointed by Privacy Commission through a notification, who shall be a person of standing, ability and integrity, qualified in the field of law and with professional experience of not less than five years, cumulatively, in one or more of the following domains:
 - (a) investigation;
 - (b) criminal procedure;
 - (c) cybercrime and cyber forensics; and
 - (d) privacy and transparency law and policy.
- (2) The number of other Additional Director General, Joint Director-General, Deputy Director-General or Assistant Directors General or such officers or other employees in the office of Data Protection, under the Director General, and the manner of their appointments, shall be such as may be prescribed by the Privacy Commission.
- (3) Every Additional Director General, Joint Director-General, Deputy Director-General and Assistant Directors General or such officers or other employees, shall exercise such powers, and discharge functions, subject to the general control, supervision and direction of the Director General.
- (4) The Additional Director General, Joint Director-General, Deputy Director-General or Assistant Directors General or such officers of other employees, shall be appointed from amongst persons of integrity, ability and standing, and who have experience in law, investigation, public administration, economics and possess such other qualifications as may be prescribed by the Privacy Commission.

Composition of the Office for Surveillance and Interception Reform of the Privacy Commission –

1. The Office for Surveillance and Interception Reform of the Privacy Commission shall consist of a Director General of Surveillance and Interception Reform, to be appointed by the Privacy Commission through a notification, who shall be a person of ability, integrity and standing, qualified in law and with professional experience of not less than five years, cumulatively, in any or more of the following domains —
 - (a) civil liberties;
 - (b) criminal procedure;
 - (c) Governmental transparency, oversight and accountability;
 - (d) police reforms.

(2) The number of other Additional Director General, Joint Director General, Deputy Director General or Assistant Directors General or such officers or other employees in the Office of Data Protection, under the Director General, and the manner of their appointments, shall be such as may be prescribed by the Privacy Commission.

(3) Every Additional Director General, Joint Director General, Deputy Director General and Assistant Directors General or such officers or other employees, shall exercise his powers, and discharge his functions, subject to the general control, supervision and direction of the Director General.

(4) The Additional Director General, Joint Director General, Deputy Director General or Assistant Directors General or such officers of other employees, shall be appointed from amongst persons of integrity, ability and standing, and who have experience in law, investigation, public administration, economics and such other qualifications as may be prescribed by the Privacy Commission.

Officers and other employees of the Privacy Commission:

1. The Privacy Commission may appoint such officers and other employees as it considers necessary for its efficient functioning under this Act.

(2) The Privacy Commission may engage such number of experts and professionals of integrity and outstanding ability, who have special knowledge of, and experience in, data, transparency, information, law, technology, economics or such other disciplines related to privacy, as it deems necessary to assist the Commission in the discharge of its functions under this Act.

(3) The salaries and allowances payable to and other terms and conditions of service of the officers and other employees of the Commission and the number of such officers and other employees shall be such as may be prescribed by the Privacy Commission.

Term of office, conditions of service, etc. of Privacy Commissioners and Offices constituted under the Commission –

1. Before appointing any person as a Chief Privacy Commissioner or Privacy Commissioner, the President shall satisfy himself that the person does not, and shall not have any such financial or other interest as is likely to affect prejudicially their functions as such Chief Privacy Commissioner or Privacy Commissioner.

(2) The Chief Privacy Commissioner and every Privacy Commissioner shall hold office for such period, not exceeding five years, as may be specified by the President in the order of his appointment, but shall be eligible for reappointment:

Provided that no person shall hold office as a Chief Privacy Commissioner or Privacy Commissioner for more than two terms:

Provided further that no person shall hold office as a Chief Privacy Commissioner or Privacy Commissioner, as the case may be, after he has attained the age of seventy-five years.

(3) Notwithstanding anything contained in sub-section (2), a Chief Privacy Commissioner or any Privacy Commissioner may —

(a) by writing under his hand and addressed to the President resign his office at any time;

(b) be removed from office in accordance with the provisions of section 53 of this Act.

(4) A vacancy caused by the resignation or removal of a Chief Privacy Commissioner or Privacy Commissioner under sub-section (3) shall be filled by fresh appointments.

(5) In the event of the occurrence of a vacancy in the office of a Chief Privacy Commissioner, such one of the Privacy Commissioners as the President may, on the advice of the selection committee under section 48(3), by notification, authorise in this behalf, shall act as the Chief Privacy Commissioner till the date on which a new Chief Privacy Commissioner, is appointed in accordance with the provisions of this Act, to fill such vacancy, enters upon his office.

(6) When a Chief Privacy Commissioner is unable to discharge his functions owing to absence, illness or any other cause, such one of the Privacy Commissioners as the Chief Privacy Commissioner may authorise in writing in this behalf shall discharge the functions of the Chief Privacy Commissioner, till the date on which the Chief Privacy Commissioner resumes his duties.

(7) The salaries and allowances payable to and the other terms and conditions of service of a Chief Privacy Commissioner and Privacy Commissioners shall be the same as that of the Chief Election Commissioner and Election Commissioners respectively:

Provided that neither the salary and allowances nor the other terms and conditions of service of a Chief Privacy Commissioner or any Privacy Commissioner shall be varied to their disadvantage after their appointment.

(8) The salaries and allowances payable to and the other terms and conditions of service of the Director General of Data Protection, the Director General of Surveillance, any Additional Director General, Joint Director General, Deputy Director General or Assistant Director General, Secretary, officer, employee appointed or expert or professional engaged shall be such as may be prescribed by the Privacy Commission.

(9) The Chief Privacy Commissioners and Privacy Commissioners on

ceasing to hold office as such shall not hold any appointment under the Government of India or under the Government of any State for a period of ten years from the date on which they cease to hold such office.

Removal of Chief Privacy Commissioners and Privacy Commissioners

1. The President may remove from office the Chief Privacy Commissioner or any Privacy Commissioner, who –
 - (a) is adjudged an insolvent; or
 - (b) engages during his term of office in any paid employment outside the duties of his office; or
 - (c) is unfit to continue in office by reason of infirmity of mind or body; or
 - (d) is of unsound mind and stands so declared by a competent court; or
 - (e) is convicted for an offence which in the opinion of the President involves moral turpitude; or
 - (f) has acquired such financial or other interest as is likely to affect prejudicially her functions as a Chief Privacy Commissioner or Privacy Commissioner, or cause some conflict of interest including benefits directly or indirectly to relatives or family members, or
 - (g) has so abused his position as to render his continuance in offence prejudicial to the public interest.
2. Notwithstanding anything contained in sub-section (1), neither a Chief Privacy Commissioner nor any Privacy Commissioner shall be removed from his office on the ground specified in clause (f) or clause (g) of that sub-section unless the Supreme Court on a reference being made to it in this behalf by the President, has on an inquiry held by it in accordance with such procedure as it may specify in this behalf, reported that the Chief Privacy Commissioner or Privacy Commissioner ought, on such grounds, to be removed.

Functions of the Privacy Commission. –

1. The Privacy Commission may, through decisions arrived at by a simple majority of its members present and voting as set out in section 59(1) of this Act, authorize, review, investigate, make an inquiry, and/or monitor, suo motu or on a petition presented to it by any person, group of persons or by someone acting on his or their behalf, the implementation and application of this Act and give such directions or pass such orders as are necessary for reasons to be recorded in writing.
- (2) Without prejudice to the generality of the foregoing provision, the Privacy Commission shall perform the following functions, namely —
 - (a) review the safeguards provided under this Act or under other laws for

the time being in force for the protection of personal data and recommend measures for their effective implementation or amendment, as may be necessary from time to time;

(b) review and/or monitor any measures taken by any competent organization, company, person or other entity for the protection of privacy and take such further action as it deems fit;

(c) authorize, review and/or monitor any action, code, certification, policy or procedure of any competent organisation, company, person or other entity to ensure compliance with the provisions of this Act and rules made hereunder;

(d) enforce the provisions of this Act at its own or on the basis of complaints received by it or by way of issuing of appropriate orders and directions, the pursuit of binding settlements with offending persons and the levy of fines;

(e) formulate, through transparent, inclusive and pervasive public consultations with experts, other stakeholders, and the general public, norms and rules for the effective protection of privacy by competent organisations, companies, persons or other entities;

(f) promote awareness and knowledge of personal data protection through any means necessary and to all stakeholders with special attention to children, including providing information to any data subject regarding their rights under this Act as requested and undertaking training and knowledge building for data controllers, including those involved in the provision of essential services and law enforcement;

(g) undertake and promote research in the field of protection of personal data and privacy;

(h) encourage the efforts of non-Governmental organisations and institutions working in the field of personal data protection and privacy;

(i) ensure the speedy and efficient redressal of all complaints, whether made by a data subject or a group of data subjects or on their behalf, whose cause of action arises on implementation of this Act;

(j) undertake efforts to facilitate international co-operation with regards to data protection, and allied subjects, including enforcement;

(k) advise the Central Government on the grant of adequacy status in respect of cross border data flows;

(l) co-ordinate in writing across State Privacy Commissions, State Governments and regulatory bodies including the Bureau of Indian Standards which may also be concerned with data protection in order to harmonize and classify standards for data including open data sets which contain personal data;

(m) such other functions as it may consider necessary for the protection of privacy, personal data, the prevention of the abuse of the criminal process, both investigatory and judicial, by the State, and enforcement of this Act;

(n) make a public, freely available publication of annual reports providing description of performance, findings, conclusions or recommendations of any or all of the functions assigned to the Privacy Commission in this Chapter.

(3) Without prejudice to the generality of the foregoing provision, the Office of Data Protection within the Privacy Commission shall perform the following functions, namely:—

(a) investigate data controllers and processors, whether initiated on complaint of a data subject or a group of them or on their behalf or on direction of the Privacy Commission or *suo motu*, for the purpose of identifying activities which are in contravention of the provisions of this Act, either at its own instance or upon receipt of credible information or complaint;

(b) obtain access from data controllers and processors, to all personal data and to all information necessary for the performance of its tasks.

(c) publish and make publicly available periodic reports concerning the incidence of compliance including violations of this Act and data breaches as reported under this Act;

(d) assist the Privacy Commission in policy formulation and other activities for effective protection of privacy;

(e) coordinate with the office for Surveillance and Interception Reform in such manner as is necessary or may be useful to the achievement of the purposes of this Act;

(4) Without prejudice to the generality of the foregoing provision, the Office for Surveillance and Interception Reform in the Privacy Commission shall perform the following functions, namely:

(a) assist the Privacy Commission in the formulation of policy and other activities for bringing about reforms in carrying out interception and surveillance by competent organization, companies, persons or other entities;

(b) collection of data from competent organizations on interception and surveillance carried out by those and analyze the same for the purpose of preparing periodic reports on compliance with provisions of this Act, including comprehensive data concerning violations of the processes of interception of communications and surveillance;

(c) advise on appointments of Public Advocates, as provided under subsection

(4) of section 70, for the purpose of defending the person being surveilled or intercepted before the Surveillance and Interception Review Division;

- (d) to appear before a Surveillance and Interception Review Divisions to provide expert evidence and testimony;
 - (e) ensure the speedy and efficient redressal of all complaints, whether made by a data subject or a group of data subjects or in their behalf, whose cause of action arises from this Act;
 - (f) co-ordinate with the office of Data Protection in such manner as is necessary or may be useful to the achievement of the purposes of this Act;
- (5) The Periodic Reports published by the Privacy Commission, stipulated under sub- section 3(c) of section 54, shall be tabled before both Houses of Parliament during the Parliamentary Session that succeeds the publication of any Periodic Report and the same shall be made publicly available, immediately thereafter.
- (6) The Chief Privacy Commissioners, Privacy Commissioners and Directors General shall appear before a special ad hoc Committee, constituted by the Speaker of the Lok Sabha and comprising of members from both the governing and the opposition parties from both Houses of Parliament, on a quarterly basis and the ad hoc Committee shall—
- (a) be empowered to review the functioning of the Privacy Commission, and may ask the Chief Privacy Commissioners and the Privacy Commissioners any questions in this regard, as per procedure of the functioning of the Committee.
 - (b) prepare and present periodic reports to both Houses of Parliament in a manner regulated by the Committee; and
 - (c) held its sitting in public in order to ensure transparency and inclusive participation.
- (7) Subject to the provisions of any rules prescribed in this behalf by the Central Government, the Privacy Commission shall have the power to review any decision, judgment, decree or order made by it.
- (8) In the exercise of its functions under this Act, the Privacy Commission shall give such directions or pass such orders as are necessary for reasons to be recorded in writing.
- (9) The Privacy Commission may, in its own name, sue or be sued.

Salaries, etc. to be defrayed out of the Consolidated Fund of India. -

1. The salaries and allowances payable to the Chief Privacy Commissioners, Privacy Commissioners, Director Generals, any Additional, Joint, Deputy or Assistant Director General, Secretary, officer, employee appointed or expert or professionals engaged and the administrative expenses of the Privacy Commission shall be defrayed out of the Consolidated Fund of India.

Vacancies, etc. not to invalidate proceedings of the Privacy Commission. –

1. No act or proceeding of the Privacy Commission shall be questioned on the ground merely of the existence of any vacancy or defect in the constitution of the Privacy Commission or any defect in the appointment of a person acting as the Chief Privacy Commissioner or Privacy Commissioner.

Chief Privacy Commissioners, Privacy Commissioners and employees of the Privacy Commission to be public servants –

1. The Chief Privacy Commissioners and Privacy Commissioners and other employees of the Privacy Commission shall be deemed to be public servants within the meaning of section 21 of the Indian Penal Code, 1860 (45 of 1860).

Location of the Privacy Commission. –

1. The Privacy Commission shall be located in New Delhi or in such other location as directed by the Chief Privacy Commissioner in consultation with the Central Government.

Jurisdiction of the Privacy Commission. –

1. Investigations or actions for enforcement may be instituted in the Privacy Commission, suo motu or on complaints made by any person, group of persons or anyone on their behalf, in respect of cases involving–
 - (a) data collection or processing by or on behalf of the Central Government;
 - (b) a conflict between two State Privacy Commissions; or
 - (c) extraterritorial transfers of data pertaining to Indian data subjects.
2. Any disputes as to jurisdiction shall be resolved in a manner that would accord the data subject the most timely and cost-effective access to redress, or promote the most timely and cost effective enforcement of the provisions of this Act.

Procedure to be followed by the Privacy Commission. –

1. Subject to the provisions of this Act, the Privacy Commission, in coordination with both Offices constituted under it, shall have power to make rules to prescribe –
 - (a) the procedure and conduct of its business;
 - (b) the delegation to one or more Privacy Commissioners of such powers or functions as the Privacy Commission may specify.

2. In particular and without prejudice to the generality of the foregoing provisions, the powers of the Privacy Commission shall include the power to determine the extent to which persons interested or claiming to be interested in the subject-matter of any proceeding before it may be allowed to be present or to be heard, either by themselves or by their representatives or to cross-examine witnesses or otherwise take part in the proceedings:

Provided that any such procedure as may be prescribed or followed shall be guided by the principles of natural justice.

3. Nothing in this section shall prevent either Office in the Privacy Commission from making rules in respect of matters of procedure exclusively concerning it.

Power relating to inquiries –

1. The Privacy Commission, including offices constituted under it, shall, for the purposes of any inquiry or for any other purpose under this Act, have the same powers as vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying suits in respect of the following matters, namely –
 - (a) the summoning and enforcing the attendance of any person from any part of India and examining him on oath;
 - (b) the discovery and production of any document or other material object producible as evidence;
 - (c) the reception of evidence on affidavit;
 - (d) the requisitioning of any public record from any court or office;
 - (e) the issuing of any commission for the examination of witnesses; and,
 - (f) any other matter which may be prescribed by the Central Government.
2. The Privacy Commission shall have power to require any person, subject to any privilege which may be claimed by that person under any law for the time being in force, to furnish information on such points or matters as, in the opinion of the Privacy Commission, may be useful for, or relevant to, the subject matter of an inquiry and any person so required shall be deemed to be legally bound to furnish such information within the meaning of section 176 and section 177 of the Indian Penal Code, 1860 (45 of 1860).
3. The Privacy Commission or any other officer, not below the rank of a Gazette Officer, specially authorized in this behalf by the Privacy Commission may enter any building or place where the Privacy Commission has reason to believe that any document relating to the subject matter of the inquiry may be found, and may seize any such document or take extracts or copies therefrom subject to the provisions of section 100 of the Code of Criminal Procedure, 1973 (2 of 1974), in so far as it may be applicable.

4. The Privacy Commission shall be deemed to be a civil court and when any offence as is described in section 175, section 178, section 179, section 180 or section 228 of the Indian Penal Code, 1860 (45 of 1860) is committed in the view or presence of the Privacy Commission, the Privacy Commission may, after recording the facts constituting the offence and the statement of the accused as provided for in the Code of Criminal Procedure, 1973 (2 of 1974), forward the case to a Magistrate having jurisdiction to try the same and the Magistrate to whom any such case is forwarded shall proceed to hear the complaint against the accused as if the case had been forwarded to him under section 346 of the Code of Criminal Procedure, 1973 (2 of 1974).

Decisions of the Privacy Commission. –

1. The decisions of the Privacy Commission shall be taken by majority and be binding and enforceable as a decree of a court as per the provisions of the Code of Civil Procedure, 1908.
2. In its decisions, the Privacy Commission has the power to:
 - (a) require a competent organisation, company, person or other entity to take such steps as may be necessary to secure compliance with the provisions of this Act;
 - (b) require a competent organisation, company, person or other entity to compensate any person for any loss or detriment suffered;
 - (c) impose penalties.

Proceedings before the Privacy Commission to be judicial proceedings. –

1. The Privacy Commission shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973 (2 of 1974), and every proceeding before the Privacy Commission shall be deemed to be a judicial proceeding within the meaning of section 193 and section 228 and for the purposes of section 196 of the Indian Penal Code, 1860 (45 of 1860).

Appeals -

1. Subject to any conditions prescribed by rules made in this regard by the Central Government, in consultation with the Attorney General of India and the Chief Justice of India, all appeals from Privacy Commission shall lie to a bench of the Supreme Court, specifically designated by the Chief Justice of India in that regard.

Chapter VI

State Privacy Commissions

State Privacy Commissions –

1. Every State Government shall, within a year of coming into force of this Act, by notification in the Official Gazette, with immediate effect, constitute a body to be known as the (name of the State) Privacy Commission to exercise the powers conferred on, and to perform the functions assigned to, it under this Act.

(2) Every State Privacy Commission shall consist of at least one Privacy Commissioner, to be appointed by the Governor of that State.

(3) Every State Government shall issue a public advertisement inviting applications to fill all vacancies in the State Privacy Commission.

(4) The selection committee for the appointment of the members of the State Privacy Commission shall be constituted by the Governor of that State and shall comprise of the—

(a) the Chief Justice and two senior most judges of the State High Court;

(b) the Law Minister of the State Government;

(c) the Leader of the Opposition or the Leader of the single largest opposition party with the greatest numerical strength in the Legislative Assembly of the State;

(d) one eminent person with experience in technology and academic or public interest research;

(e) representing the private sector; and

(f) one eminent person representing the civil society.

(5) All proceedings of the selection committee shall be matters of public record.

Explanation.—The term 'Civil Society' means non-Governmental and non-profit organisations that engage in the activities for the general upliftment and interests of the people in the field of privacy and is independent of Government funding, interference or influence.

(4) No Members of Parliament or Members of the Legislature of any State or Union territory having Legislative Assembly or a member of any political party shall be eligible for selection or appointment as a State Privacy Commissioner and persons holding any other office of profit or carrying on any business or practicing any profession, before he enters upon this office, may be selected or appointed as State Privacy Commissioner, as the case may be, if—

(a) he holds any office of trust or profit, resigns from such office; or

(b) he is carrying on any business, severs his connection with the conduct and management of such business; or

(c) he is practicing any profession, ceases to practice such profession.

(5) 'Except as provided for expressly under this Act, a State Privacy Commission shall have powers and functions coequal and identical to those of the Privacy Commission in all respects.

(6) A State Privacy Commission may appoint such officers and other employees, or engage any professional or expert, as it considers necessary for the efficient performance of its functions under this Act.

(7) Every State Privacy Commission shall be autonomous, independent, and free from external interference and shall be provided with sufficient operational resources including human, technical, and financial for the effective discharge of its duties and exercise of its powers.

(8) The financial power of Privacy Commission shall be subject to audit by the Comptroller and Auditor General of India.

(9) The salaries and allowances payable to and the other terms and conditions of service of State Privacy Commissioners shall be the same as that of the Chief Secretary to the State Government.

(10) The salaries and allowances payable to and the other terms and conditions of service of any officer, employee appointed or expert or professional engaged shall be such as may be prescribed by the State Privacy Commission.

Jurisdiction of the State Privacy Commissions. –

1. Investigations or actions for enforcement may be instituted in the State Privacy Commission, suo motu or on complaints made by, any person, group of persons or anyone on their behalf, within the local limits of whose jurisdiction –

- (a) the complainant or data subject actually and voluntarily resides;
- (b) where the data controller or data processor is physically located or principally carries out business; or
- (c) the cause of action, wholly or in part, arises.

2. Any disputes as to jurisdiction shall be resolved in a manner that would accord the data subject the most timely and cost-effective access to redress, or promote the most timely and cost effective enforcement of the provisions of this Act.

Appeals. –

1. Subject to any conditions prescribed by rules made in this regard by appropriate State Government, all appeals from a State Privacy Commission shall lie to a bench of the respective High Court, specifically designated by the Chief Justice in that regard.
2. Notwithstanding sub-section (1), appeals from a State Privacy Commission shall lie to the Privacy Commission where -
 - (a) there is a dispute as to jurisdiction between two or more State Privacy Commissions; or
 - (b) two or more State Privacy Commissions have passed orders or directions, or otherwise taken any action in respect of the same cause of action

Provided that in any such appeal, the Privacy Commission shall be included as a necessary party.

Procedure. -

1. The State Government shall, in consultation with its Advocate General, the Chief Justice of its High Court and the Privacy Commission, prescribe rules governing the procedures to be followed:
 - (a) by and before the State Privacy Commission, and
 - (b) in respect of appeals to its High Court in terms of sub-section (1) of section 67.

Power to make rules. -

1. Subject to the provisions of this Act, every State Government may, in consultation with the State Privacy Commission, by notification in the Official Gazette, prescribe rules in order to bring into effect any of the provisions of this Chapter of the Act.

Chapter VII

Surveillance and Interception Review Divisions

Surveillance and Interception Review Divisions. -

1. The Central Government shall, by notification in the Official Gazette, constitute, within a period of six months from the enactment of this Act, a division in every High Court to be known as the Surveillance and Interception Review Division, hereinafter referred to as the Division:

Provided that if the Division is not constituted within the stipulated time period, no order for interception or surveillance issued after a period of ninety days from the date of the stipulated time period for constitution of

the Division gets over, shall be valid and any interception or surveillance carried out under such an order shall be a violation of the provisions of this Act:

Provided further that if the Division is not constituted within the stipulated time period and till the time it is constituted, no existing order of surveillance or interception can be renewed.

(2) The Central Government shall appoint, for a period of two years or till the retirement of the Judge so appointed, whichever is earlier, two or more Judges of the High Court, as publicly designated by the Chief Justice of that High Court in consultation with the appropriate State Government, as the Division.

(3) The Central Government shall make available to the Division such information as may be necessary for the discharge of its functions under this Act.

(4) Subject to the provisions of this Act, one or more Public Advocates, shall be appointed by the Chief Justice of the High Court of that State, in consultation with the Office for Surveillance and Interception Reform of the Privacy Commission, the respective State Privacy Commission, the State Legal Services Authority, and the Bar Council of that State, for the purpose of defending the interests of the person being surveilled or intercepted, ensuring compliance with the provisions of this Act, and advancing legal arguments that further the protection of privacy and other fundamental rights under the Constitution:

Provided that while in appointing one or more Public Advocates, the Chief Justice of the High Court of the State shall do so after issuing public notice inviting applications of interest and a person shall be qualified to be appointed a Public Advocate to the Division if he—

(a) is a citizen of India, qualified to practice law with at least seven years' experience at the bar; and

(b) has experience with litigation on fundamental rights, criminal law and procedure, military and policing powers and oversight, and communications and information technology laws;

(5) The Public Advocate appointed, sub-section (4), shall—

(a) be provided copies of all ordinary applications made to and Government orders shared with the Division under this Act, including their supporting documents and filings;

(b) have a right to attend, be heard, and to file briefs and other filings before all proceedings of the Division; and

(c) be empowered to file appeals with respect to orders of the Division to the Supreme Court as provided for under this Act:

Provided that any decision not to file an appeal shall be made only after a legal opinion on the merits of the case and the decision for reasons recorded in writing which shall be made available along with the complete case files including all pleadings and materials when the disclosure of the orders of the Surveillance and Interception Review Division are made as per the provisions under the Act.

(6) All expenses incurred in connection with the Division shall be defrayed out of the Consolidated Fund of India.

(7) Subject to any rules made in this regard by the Central Government, in consultation with the Privacy Commission, the Division shall have power to regulate its own procedure in all matters arising out of the discharge of its functions including.

(8) The rules framed under sub-section (7), may provide for inner-camera proceedings of the Division, the manner in which third parties interested in the matter may make application for attending the hearings before the Division, for making the decisions of the Division public after a stipulated time period not exceeding one year since the date of the order and other incidental matters.

(9) The Division shall, for the purpose of making an inquiry under this Act, have the same powers as are vested in a Civil Court under the Code of Civil Procedure, 1908 while trying a suit, in respect of the following matters, namely:—

(a) the summoning and enforcing the attendance of any witness and examining him on oath;

(b) the discovery and production of any document or other material object producible as evidence;

(c) the reception of evidence on affidavits;

(d) the requisitioning of any public record from any court or office;

(e) the issuing of any commission for the examination of witnesses.

(10) Any proceeding before the Division shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228 of the Indian Penal Code, 1860 and the Division shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code.

(11) Subject to provisions of this Act, the Director General of Surveillance and Interception Reform constituted under the Privacy Commission, shall have access to the proceedings of the Division in order to assist the Division by providing expert evidence, legal arguments, and testimony.

Appointment, terms of service, etc. –

1. Terms of service, removal and allied matters relating to persons appointed to the Tribunal shall be governed by rules made in this regard by the Central Government, in consultation with Privacy Commission and appropriate State Government.

Provided that no terms and conditions of service of persons appointed to the Tribunal shall be varied to their disadvantage after their appointment.

Jurisdiction of the Surveillance and Interception Divisions. –

1. Subject to the provisions of Chapter IV of this Act, the Tribunal, which shall review, renew or take any other action with respect to orders of surveillance or interception, shall be the Tribunal within the local limits of whose jurisdiction –
 - (a) the person to be surveilled or intercepted actually and voluntarily resides;
 - (b) where the competent organization seeking to undertake surveillance or interception is physically located; or
 - (c) where the actual act of interception or surveillance is to be carried out.

Appeals -

1. Subject to any conditions prescribed by rules made in this regard by the Central Government, in consultation with the Privacy Commission, and the appropriate State Governments, all appeals from any of the Tribunals shall lie to a bench of the Supreme Court, specifically designated by the Chief Justice of India in that regard

chapter ix

Offences and penalties

Punishment for offences related to personal data. –

1. Whoever, except in conformity with the provisions of this Act, collects, receives, stores, processes, discloses or otherwise handles any personal data shall be liable to fine which may extend up to one hundred crore rupees based on the proportionality of the harm caused.
 - (2) Whoever commits the offence under sub-section (1) either intentionally, or with reckless disregard, he shall be liable for a term of imprisonment extending upto three years, and shall also be liable to fine:

Provided further that in case of companies, the penalty shall be governed by section 78.

(3) Whoever attempts to commit any offence under sub-section (1) shall be liable in the manner and to the extent provided for such offence under that sub-section.

(4) Whoever, except in conformity with the provisions of this Act, collects, receives, stores, processes, discloses or otherwise handles any sensitive personal data shall be liable to fine which may extend to two hundred crore rupees:

Provided that whoever commits the offence either intentionally, or with reckless disregard, he shall be liable for a term of imprisonment extending upto five years, and shall also be liable to fine:

Provided further that in case of offence committed by companies, the penalty shall be governed by section 78.

(5) Whoever attempts to commit any offence under sub-section (3) shall be punished with imprisonment and fine as provided for such offence in that section.

Punishment for offences related to interception of communication –

1. Whoever, except in conformity with the provisions of this Act, intercepts, or causes the interception of, any communication of another person shall be liable to a fine which may extend to one hundred crore rupees:

Provided that whoever commits the offence under sub-section (1) either intentionally, or with reckless disregard, shall be liable for a term of imprisonment extending up to three years, and shall also be liable to fine.

(2) Whoever attempts to commit any offence under sub- section (1) shall be punished with imprisonment and fine as provided in that sub-section.

Punishment for offences related to surveillance –

1. Whoever, except in conformity with the provisions of this Act, orders or carries out, or causes the ordering or carrying out, of any surveillance of another person shall be liable to a fine which may extend to ten crore rupees:

Provided that whoever commits the offence defined above either intentionally, or with reckless disregard, shall be liable for a term of imprisonment extending upto five years, and shall also be liable to fine.

(2) Whoever attempts to commit any offence under sub- section (1) shall be punished with imprisonment and fine as provided in that section.

Abetment and offenders –

1. Whoever abets any offence punishable under this Act shall be punished with imprisonment or fine, as the case may be, provided for that offence.

Offences by companies –

1. Where an offence under this Act has been committed by a company, every person who, at the time of the offence was committed, was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to any punishment, if he proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence.

2. Notwithstanding anything contained in sub-section (1), where any offence under this Act has been committed by a company and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any neglect on the part of any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall be deemed to be guilty of that offence, and shall be liable to be proceeded against and punished accordingly.

Cognizance –

1. Notwithstanding anything contained in the Code of Criminal Procedure, 1973, the offences under this chapter shall be cognizable and non-bailable.

General penalty for failure to comply with notice or order issued under this Act –

1. Whoever, in any case in which a penalty is not expressly provided by this Act, fails to comply with any notice or order issued under any provisions thereof, including an order of the Chief Privacy Commissioner or otherwise contravenes any of the provisions of this Act, shall be punishable with fine which may extend to one crore rupees, and, in the case of subsequent contravention, with an additional fine which may extend to ten lakh rupees for every day.

Punishment to be without prejudice to any other action –

1. The award of punishment for an offence under this Act shall be without prejudice to any other action which has been or which may be taken under this Act with respect to such contravention.

chapter X

Miscellaneous

Power to make rules –

1. The Central Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act until such time as the Privacy Commission is constituted.
 - (2) The Privacy Commission may, by notification in the Official Gazette, make rules to carry out the provisions of this Act:

Provided that where the Privacy Commission makes rules upon a subject already covered by the Central Government, it shall ensure that protections accorded to data subjects by its rules are maintained or improved.

 - (3) In particular, and without prejudice to the generality of the foregoing powers, such rules may provide for such measures as may be necessary to secure—
 - (a) all personal data related to data subjects located in India; and
 - (b) any personal data flowing into and out of, exported or imported out of India;
 - (c) the notification of theft, loss or damage under sub-section (4) of section 17;
 - (d) the notification of disclosure under sub-section (5) of section 19;
 - (e) the application by an intelligence organisation under sub-section (1) of section 31;
 - (f) the application to intercept a communication under sub-section (1) of section 28;
 - (g) the application to renew an interception of communication under sub-section (2) of section 33;
 - (h) the notification of an interception of communication under sub-section (1) of section 34;
 - (i) the application to not inform under sub-section (2) of section 34;
 - (j) the application to store information obtained as a result of any interception of communication under sub-section (2) of section 37;
 - (k) the application to carry out surveillance under sub-section (3) of section 39;
 - (l) notification to the general public under sub-section (2) of section 40; the application to renew surveillance under sub-section (2) of section 41;
 - (m) the notification of surveillance under sub-section (1) of section 42;
 - (n) the application to not inform under sub-section (2) of section 42;
 - (o) the application to store information obtained as a result of surveillance under sub-section (2) of section 45;

(p) salaries, allowances and other terms and conditions of service of the Chief Privacy Commissioner, Privacy Commissioners, Secretaries and other members, staff and employees of the Privacy Commission;

(q) procedure to be followed by the Privacy Commission;

(r) powers and duties of Secretaries, officers and other employees of the Privacy Commission; and

(s) the effective implementation of this Act.

(4) Every rule made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament while it is in session for a period of thirty days which may be comprised in one session or in two successive sessions and if before the expiry of the session in which it is so laid or the session immediately following, both Houses agree in making any modification in the rule, or both Houses agree that the rule should not be made, the rule shall thereafter have effect only in such modified form or be of no effect, as the case may be, so however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule.

(5) Every rule made by the Central Government under sub-section (1) shall require express assent of both Houses of Parliament:

Provided that where assent under sub-section (5) is not obtained, the rules shall not be valid.

Bar of jurisdiction –

1. On and from the appointed day, courts or authorities shall have, or be entitled to exercise jurisdiction with respect to remedies provided for data subjects and against data subjects under this Act with respect:

Provided that legal proceedings for relief in the nature of interim injunctions or mandatory injunctions shall not be initiated against the authorities provided for under this Act including but not limited to the State Privacy Commission and the Privacy Commission:

Provided that further provisions of the Arbitration and Conciliation Act, 1996 shall not bar the Privacy Commission or the State Privacy Commission or any other body from exercising jurisdiction under the provisions of this Act.

(2) No order passed under this Act shall be appealable except as provided therein and no injunction shall be granted by any court or Division to any authority established under this Act in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

Protection of action taken in good faith –

1. No suit or other legal proceeding shall lie against the Central Government, State Government, Privacy Commission, Chief Privacy Commissioner, Privacy Commissioner or any person acting under the direction either of the Central Government, State Government, Privacy Commission, Chief Privacy Commissioner or Privacy Commissioner in respect of anything which is in good faith done or intended to be done in pursuance of this Act or of any rules or any order made thereunder.
2. Notwithstanding anything inconsistent therewith contained in any other law for the time being in force any communication or complaint made in good faith made by any person alleging violation of the provisions of this act, if made to the Privacy Commission, the Surveillance and Interception Review Divisions and their Public Advocates, or to any High Court or the Supreme Court, shall not be treated as a violation of this Act or any other law.

Power to remove difficulties –

1. If difficulty arises in giving effect to the provisions of this Act as provided for under this section, the Central Government may, by order, published in the Official Gazette, make such provisions, not inconsistent with the provisions of this Act, as appears to it to be necessary or expedient for removing the difficulty:

Provided that no such order shall be made under this section after the expiry of a period of three years from the commencement of this Act.

2. The provisions of sub-section (1) shall only apply in instances when it is with respect to conflict between this Act and any existing law;
3. Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

Act to have overriding effect –

1. Except as otherwise provided in this Act, the provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force, including provisions in—
 - (a) sections 43A, 69, 69B, 72 and 72A of the Information Technology Act, 2000;

and

 - (b) sections 7, 28, 29, 30, 31, 32, 33 and 47 of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016;

and

- (c) section 5(2) of the Indian Telegraph Act, 1885; and
- (d) section 21 of the Prevention of Money Laundering Act, 2002; and The Census Act, 1948.

(2) Nothing contained in sub-section (1) shall apply to the provisions of the Representation of the People Act, 1951 and the Right to Information Act, 2005.

(3) Where the provisions of any law in force provide for additional safeguards that are not inconsistent with the present Act, those provisions shall continue to apply and the Act shall not be considered in derogation of such provisions.

THE SCHEDULE

Competent Organisations

[See Section 2(i)]

(1) 'Armed force' to mean any body raised or constituted pursuant to or in connection with, or presently governed by, the Army Act, 1950 (46 of 1950), the Indian Reserve Forces Act, 1888 (4 of 1888), the Territorial Army Act, 1948 (6 of 1948), the Navy Act, 1957 (62 of 1957), the Air Force Act, 1950 (45 of 1950), the Reserve and Auxiliary Air Forces Act, 1952 (62 of 1952), the Coast Guard Act, 1978 (30 of 1978) or the Assam Rifles Act, 2006 (47 of 2006).

(2) 'Intelligence Organisation' to mean an intelligence organisation under the Intelligence Organisations (Restriction of Rights) Act, 1985 (58 of 1985) as on the date of this Act receiving Presidential assent.

(3) 'Police Force' mean

(a) any body raised or constituted by the appropriate Government for the preservation of law and order and enforcement of laws related to customs, revenue, foreign exchange, excise, income tax and narcotics;

(b) the bodies raised or constituted pursuant to or in connection with, or presently governed by, the Police Act, 1861 (5 of 1861), the Central Reserve Police Force Act, 1949 (66 of 1949), the Border Security Force Act, 1968 (47 of 1968), the Indo- Tibetan Border Police Force Act, 1992 (35 of 1992), the Sashastra Seema Bal Act, 2007 (53 of 2007), the Central Industrial Security Force Act, 1968 (50 of 1968), the Railway Protection Force Act, 1957 (23 of 1957) and the National Security Guard Act, 1986 (47 of 1986);

(c) the bodies raised or constituted pursuant to or in connection with, or presently governed by, the Delhi Special Police Establishment Act, 1946 (25 of 1946), the Income Tax Act, 1961 (43 of 1961), the National Investigation Agency Act, 2008 (34 of 2008) and the Central Vigilance Commission Act, 2003 (45 of 2003);

- (d) The National Investigation Agency constituted under sub-section (1) of section 3 of the National Investigation Agency Act, 2008 (34 of 2008).
- (e) Any police forces raised or constituted by the States, armed or otherwise.

STATEMENT OF OBJECTS AND REASONS

1. The Supreme Court, in a landmark judgment has affirmed the fundamental right to privacy. Such a verdict requires a comprehensive law to safeguard the privacy of citizens.

In his notes accompanying the clauses of a draft Bill of Rights, Dr. Ambedkar noted that:

“The purpose is to protect the liberty of the individual from invasion by other individuals which is the object of enacting fundamental rights. The connection between individual liberty and the shape and form of the economic structure of society may not be apparent to everyone. Nonetheless the connection between the two is real. It shall be apparent if the following considerations are borne in mind. Political democracy rests on four premises which may be set out in the following terms:—

1. the individual is an end in himself;
2. that the individual has certain inalienable rights which must be guaranteed to him by the Constitution;
3. that the individual shall not be required to relinquish any of his constitutional rights as a condition precedent to the receipt of a privilege; and
4. that the State shall not delegate powers to private persons to govern others.”

The Bill covering data protection and surveillance reform empowers citizens by providing autonomy and dignity through the right to privacy. The Bill creates a strong and independent Privacy Commission to enforce the right to privacy via investigation, rule-making and adjudication.

This Bill has been drafted keeping in mind global best practices, report of the Justice A.P. Shah Committee of Experts and submissions by multiple lawyers to the Justice Srikrishna Committee of Experts. The Bill has been significantly updated and incorporated best practices from international texts such as the European Union’s General Data Protection Regulation.

The Bill is based on principles of individual rights, data protection, user privacy, surveillance reform, and a free and open internet. The respect for individual rights is at the core of the Personal Data and Information

Privacy Code Bill, which maintains access Right to Information while also enabling citizens to safeguard their privacy.

NEW DELHI;

D. RAVIKUMAR

June 26, 2019.

FINANCIAL MEMORANDUM

1. Clause 47 of the Bill provides that the Central Government shall constitute a Privacy Commission to perform the functions and duties assigned to it under this Act. Clause 48(1) provides for appointment of Privacy Commissioners to the Privacy Commission. Clause 48(3) provides for the appointment of a Selection Committee to fill the vacancies in the Privacy Commission. Clause 51(1) provides for appointment of officers and employees by the Central Government to the Privacy Commission. Clause 51(2) provides for salaries and allowances payable to such employees or officers of the Privacy Commission. Clause 52(7) provides for salaries and allowances payable to Chief Privacy Commissioners and Privacy Commissioners of the Privacy Commission. Clause 55 provides for Central Government to provide requisite funds to the Privacy Commission through the Consolidated Fund of India.

Clause 65 provides for constitution of State Privacy Commission by the State Governments. Clause 65(6) provides for appointment of officers and employees by the State Government to the State Privacy Commission. Clause 65(7) provides for State Government to provide requisite funds to the State Privacy Commission. The expenditure relating to States shall be borne out of the Consolidated Funds of State Governments concerned. Clause 65(9) provides for salaries and allowances payable to State Chief Privacy Commissioners and Privacy Commissioners of the State Privacy Commission.

However, the expenditure relating to Union territories shall be borne out of the Consolidated Fund of India. The Bill, therefore, if enacted would involve expenditure from the Consolidated Fund of India. It is estimated that a recurring expenditure of about rupees five hundred crore per annum would involve from the Consolidated Fund of India.

A non-recurring expenditure of about rupees two hundred crore is also likely to be involved.

MEMORANDUM REGARDING DELEGATED LEGISLATION

1. Clause 82 of the Bill empowers the appropriate Government to make rules for carrying out the purposes of the Bill. As the rules will relate to matters of detail only, the delegation of legislative power is of a normal character.



Telecom Regulatory Authority of India

Recommendations

on

Privacy, Security and Ownership of the Data in the Telecom Sector

New Delhi

16th July 2018

Telecom Regulatory Authority of India

Mahanagar Doorsanchar Bhawan,

Jawahar Lal Nehru Marg,

New Delhi-110002

www.trai.gov.in

Index

Chapter	Topic	Pages
1	Introduction	1-7
2	Data Protection Framework	8-67
3	Summary of Recommendations	68-73
	List of Abbreviations	74-75

Chapter-1: Introduction

- 1.1 Telecommunications has been an important growth engine in the development of modern India. It has enabled connectivity to the remotest corners of the nation which has not only benefited the citizens but also helped in better governance. Access to digital services and applications from remotest parts of the country is enabled by telecommunication connectivity. As per a study¹ doubling of mobile data usage increases the GDP by 0.5% points while a 10% increase in mobile telecom penetration increases Total Factor Productivity in long run by 4.2% points. As per a report on statistics of internet usage in India² there are total 462.1 million internet users (approx 34% of population, global average is 53%) out of these, 282 million are active internet users spending approximately 7 hours per day on the internet. Out of total 462.1 million internet users, 430.3 million use the internet from mobile phones (79% of the total web traffic). Active social media penetration in India is 19% of the total population; global average is 42% of the total population. A user spends approximately 2 hours 30 minutes daily on social media and has on an average seven mobile applications being used on his mobile device.
- 1.2 The eco-system used for delivery of digital services consists of multiple entities like Telecom Service Providers (TSPs), Personal Devices (Mobile Handsets, Tablets, Personal Computers etc), M2M (Machine to Machine) Devices, Communication Networks (consisting of Base Trans Receiver Stations, Routers, Switches etc), Browsers, Operating Systems, Over The Top (OTT) service providers, Applications etc. It is estimated that the global volume of digital data created annually was 4.4 zettabytes in 2013 and this would reach 44 zettabytes by 2020³. Further, it is expected that the number of devices connected to the IP

¹ <https://www.gsma.com/publicpolicy/wp-content/uploads/2012/11/gsma-deloitte-impact-mobile-telephony-economic-growth.pdf>

² 2018 Global Digital Report by We Are Social & Hootsuite

³ The Digital Universe of Opportunities: Rich Data and the Increasing Values of the Internet of Things', EMC Digital Universe with Research and Analysis by IDC (April 2014), available at:<https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.html>

Networks would be approximately three times the global population by 2021⁴. The growth in the number of connected devices imply that a large portion of data created would presumably consist of personal details relating to individuals, e.g purchases, places visited, demography, health statistics, financial transactions, education, work profile etc

- 1.3 Enterprises around the world have realized the value of user data; hence technologies are being developed for more accurate sifting of data and better understanding of consumer's requirements⁵. Enhancement in the computational powers of modern computers coupled with the rapid development of technology has made it possible to process voluminous data in order to identify correlations and discover patterns in all fields of human activity which can be utilized even for profiling. Data of individuals can be utilized for problem solving, ensuring targeted delivery of benefits, and bring new products and services to the market etc.
- 1.4 Technology, though beneficial to the mankind in general, does have collateral disadvantages e.g. increasing use of smart devices in everyday lives can lead to a loss of privacy for individuals, who may often not even be aware that they are being tracked or observed. Similarly, ubiquitous presence of smart devices like a mobile handset has many benefits but it may also be a source of loss of privacy of the user, e.g. when a user knowingly/unknowingly grants permission to access the camera and micro phone of a smart device to an application; the application may execute live streaming on the internet using camera and micro phone, run real time facial recognition algorithms, use advanced algorithms to create a three dimensional model of the users face, upload random frames of video stream being

⁴ <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html>

⁵ 10 Key Marketing Trends for 2017 and Ideas for Exceeding Customer Expectations, IBM, <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WRL12345USEN>.

accessed by the user etc. Data collated by such applications over a period of time may be utilized for predictive profiling of the individual which may seriously jeopardize the data privacy of the users.

- 1.5 As stated earlier, Digital services and applications are accessed using telecommunication connectivity. When a user accesses an online application or social media website, the data generated passes through the telecom network. It is therefore vital that user privacy is ensured appropriately in the telecommunications layer - both from external agents who may wish to cause harm to users (for instance, by stealing their personal data for purposes of fraud) and from entities in the telecom space who may wish to (mis)use user data that they have access to (for instance in the form of unsolicited targeted advertising). It is worth reiterating that Telecom Service Providers (TSPs) control the "pipes" through which information is exchanged. Due to increasing computing power, TSPs may have an increased ability to analyse the contents of the pipe i.e. the data flow of users, leading to obvious privacy concerns. In addition to TSPs, the widespread adoption of smart devices amongst the populace is also a trend that must be considered. Unlike in the past, when the intelligence was residing in the telecommunication networks only and user devices were not intelligent, now, smart devices (including Operating systems, Browsers, Applications etc) are increasingly playing a gate-keeping role over the network: they determine how users connect to and experience a network. As with TSPs, all user data flows through these smart devices, putting the Device Manufacturers, Browsers, Operating Systems, and Applications etc. in a prime position to collect and process the personal information of users. Given that all user data has to pass through the TSPs (analogous to pipes) and devices (analogous to faucets) it is essential that appropriate steps are taken to protect user privacy vis-a-vis these entities. In effect, the subject of data ownership, privacy, and security is multi-dimensional and

complex, and hence data consumers must be empowered to navigate safely and securely through the maze of the digital eco-system.

- 1.6 As the economy increasingly moves to the digital/online world, it is all the more important that users are appropriately protected from all entities in the ecosystem that may seek to take advantage of their gate-keeping power. A failure to adequately protect users from the very real possibility of harm (caused by the loss of privacy) may result in restricting the growth of the entire digital economy which include telecommunication services also.
- 1.7 Given the Authority's mandate to ensure user protection in the telecommunications space, it is essential that appropriate norms be laid out for privacy and protection of telecommunication consumers. Accordingly, with a view to bring out the multiple aspects of the data protection in the telecommunication sector, and to provide a suitable platform for discussion, TRAI issued a consultation paper (CP) on "Privacy, Security and Ownership of the Data in the telecom sector" on 09 August 2017. The objective of the CP was to identify the key issues pertaining to data protection in relation to the delivery of digital services through the telecommunication systems. Written comments on the CP were invited from the stakeholders. An Open House Discussion (OHD) was also conducted on 01st February 2018 at New Delhi. Based on the written submissions of the stakeholders and the discussions in the OHD, the issues have been examined in depth and recommendations have been framed.
- 1.8 The recommendations are also to be viewed in the light of the details in the following two paragraphs:
 - (a) In 2016, the Department of Telecommunications (DoT) sought the recommendations of the Authority on three aspects related to M2M communications (quality of service, roaming requirements and spectrum requirements). In its Consultation Paper on Spectrum, Roaming, and QoS related requirements in

M2M Communications (October 18, 2016, CP No. 21/2016), the Authority also raised issues pertaining to the privacy and security of M2M communications (apropos of which it received numerous responses from stakeholders). Pursuant to consultations and an analysis of responses, the Authority issued recommendations related to M2M communications on September 5, 2017. These recommendations however did not address the issues pertaining to privacy and security of M2M communications as it was decided to address them separately. In view of the similarity of issues raised in the CP on Privacy, Security and Ownership of Data and the issues pertaining to privacy and security of M2M communications, the present recommendations deal with both sets of issues in a holistic manner.

- (b) On 24th August 2017, a nine-judge bench of the Supreme Court in Justice K.S. Puttaswamy vs Union of India unanimously recognized the constitutional right to privacy rooted in human dignity and individual autonomy. The Court declared that privacy constitutes an intrinsic part of the right to life and personal liberty under Article 21. It was recognized that privacy is a multidimensional construct encapsulating within it various rights such as informational privacy, bodily-integrity, and self-determination. The Court also noted both the positive and negative obligations arising out of the fundamental right to privacy and the dangers faced from private actors. The Court clarified that the right to privacy is not absolute and that the state can place reasonable restrictions on it in the interest of fulfilling objectives such as protecting national security,

preventing and investigating crime, encouraging innovation, and preventing the dissipation of social welfare benefits⁶.

- 1.9 The Government is also seized of the matter concerning the privacy of data of users. It constituted a Committee of Experts on 31 July 2017, under the Chairmanship of Justice B N Srikrishna, Former Judge, Supreme Court of India to identify key data protection issues in India and recommend methods of addressing them. The terms of reference for this Committee are as follows:
 - (a) To study various issues relating to data protection in India.
 - (b) To make specific suggestions for consideration of the Central Government on principles to be considered for data protection in India and suggest a draft data protection bill.
- 1.10 The Authority is of the view that the larger issues relating to data protection framework applicable in general for all sectors of the economy would in any case be addressed by the Committee of Experts headed by Justice B N Srikrishna. TRAI, in its present recommendations has considered only the TSPs - which provide the connectivity and communication services; devices - which an end user uses to access the network and services; and the users of telecommunication services themselves. Further, the Authority is cognizant of the fact that the present recommendations may require updating /revision pursuant to introduction of a new data protection law/framework in the country. Once the data protection Law is enacted, the Authority may revisit the issue again in the specific context of the telecommunication sector.
- 1.11 The issues relating to data protection framework raised in the CP, responses received from the stakeholders, analysis, and the recommendations have been covered in Chapter 2. The responses

⁶ Bhandari, Kak, Parsheera and Rahman, An analysis of Puttaswamy: the Supreme Court's privacy verdict, available at <https://ajayshahblog.blogspot.in/2017/09/an-analysis-of-puttaswamy-supreme.html>.

were widely divergent and the Authority has taken a holistic view of the different facets of privacy, security, and ownership of data to arrive at the recommendations. The summary of recommendations has been provided in Chapter 3.

CHAPTER 2: Data Protection Framework

- 2.1 The Digital Eco-system comprises of multiple entities like Devices (Mobiles, Laptops, Tablets, PCs etc), Telecom Service Providers (TSPs), Communication Networks (consisting of Switches, Routers, Base Trans-Receiver Stations etc), Browsers, Operating Systems, Applications, Over The Top (OTT) service providers, M2M devices etc. Most of these entities have capability of gate-keeping function, and an asymmetric advantage of accessing, collecting, and collating users' data. Thereby these entities could infringe upon the privacy of users. It is therefore important to ensure that the data is collected, stored, and processed in regulated manner with the informed and explicit consent of users.
- 2.2 In the backdrop of possible threats to the data privacy of the telecommunication consumers, the Authority raised the following issues in the CP, for obtaining the views of the stakeholders-
- (a) Examine the present definition of personal data, and in light of recent advances in technology, suggest changes, if any.
 - (b) Sufficiency of existing data protection laws applicable to all the players in the digital ecosystem and additional measures, if any, which may be required to strengthen the framework.
 - (c) Identification of key issues of data protection pertaining to collection of data by various stakeholders in the digital ecosystem and measures that needs to be taken to address those issues.
 - (d) Examining the need to bring parity in data protection norms applicable to the TSPs and other communication service providers offering comparable services.
 - (e) Rights and responsibilities of Data Controllers and the suggested mechanism to regulate the Data Controllers.

- (f) Need to establish a technology enabled architecture to audit use of personal data, and monitor the entire digital eco-system for compliance.
- (g) Measures that need to be considered to strengthen the safety and security of telecom infrastructure and the digital eco-system as a whole.
- (h) Measures to be undertaken to encourage creation of new data based businesses.
- (i) Need for setting up Data Sandboxes by the government for development of newer services.
- (j) Examine the legitimate exceptions to the data protection requirements imposed on TSPs and other stakeholders in the digital eco-system.
- (k) Identifying and examining the potential issues arising from cross border data flow and measures that need to be considered to address them

A. Personal Data

- 2.3 Every time, a large quantity of data is generated when an individual/machine comes into contact with the digital ecosystem. Data generated may include information relating to an individual, meta-data, as well as M2M communication data that relates to an individual. The modes of collecting such data are changing rapidly as well as the uses that such data can be put to.
- 2.4 Accordingly, and in view of the need to ensure a proper understanding of the term ‘personal data’, the Authority requested responses on the issue of defining personal data.
- 2.5 In response, a large number of the respondents were of the view that the existing definition of personal data provided under the sensitive

Personal Data and Information (SPDI) Rules, 2011 is sufficient and should not be changed. They were of the view that the difference between personal information, non-personal, and aggregate information should be considered during framing of laws. Also, aspects of purpose, context, and proportionality are important in determining the classification of information. Different kinds of data that can be potentially personal should be treated differently depending on the risk that certain data poses to privacy. They had further submitted that certain types of data may be benign in one context, but when combined with other forms of data this may no longer be the case.

- 2.6 One stakeholder was of the view that technology changes occur at a very rapid pace. Hence, the regulatory framework should match or account for the pace of technical advancement. The current SPDI Rules were published in 2011 and ever since no amendment has been made. However, since 2011 there have been numerous technological changes especially in the social networking and M2M services domain; and that enable collection of large quantities of personal information about an individual. The information so generated has the ability to clearly identify an individual and, hence, there is a need to enlarge the list of information relating to an individual defined under SPDI Rules.
- 2.7 Some stakeholders submitted that:
 - (a) Personal data should also include: Online activity, information stored in personal devices, information obtained from personal use of M2M devices, personal details, family, lifestyle and social activities, employment details, financial details, goods or services procured etc.
 - (b) The scope and ambit of personal data should be widened so as to cover data secured by broadband service providers; mobile set manufacturers, device and software appliance developers.

- 2.8 Some stakeholders were of the view that new data protection framework, should not be overly restrictive for the data analytics industry by framing stringent definitions of personal data or incorporating mechanisms that are deterrent to the growth of the data industry. Entities operating in the digital ecosystem may be subjected to privacy rules of the country in which services are being offered.
- 2.9 Some other respondents were of the view that while defining personal data no distinction should be made with respect to the source of data. For instance, the data generated by a smart device and the data generated while availing telecom services should be subjected to same regulatory framework.
- 2.10 A few stakeholders were of the view that anonymous data is not personal data and, therefore, anonymised data may be accorded simpler, less stringent privacy protections. Only anonymised and aggregated data should be allowed to be used by companies for developing better services/products. Further, since anonymised data cannot be used to identify and locate/profile/track any individual, it should not be included under the definition of personal data. They were also of the view that pseudonymisation can provide safeguards to user data and hence it may be considered while framing the data privacy framework for the country.
- 2.11 In contrast to the above-mentioned submission, some stakeholders were of the view that complete anonymization of data is not achievable. Further, the respondents cited two research reports, one from the University of Texas⁷ and the other from the Colorado Law Legal Studies Research⁸ which showed the possibility of re-identification of users from the anonymised data sets. Thus, sufficient

⁷ Narayanan, A. and Shmatikov, V, Robust De-anonymization of Large Sparse Datasets, available at https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf

⁸ Ohm, Paul, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (August 13, 2009). UCLA Law Review, Vol. 57, p. 1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12. Available at SSRN: <https://ssrn.com/abstract=1450006>

safeguards in the form of anonymization guidelines and standards are necessary if such a distinction is created including the prohibition of de-anonymization subject to stringent penalization. They were of the opinion that metadata should be accorded the same protection as applicable to personal data. They also submitted that metadata should not be used by the TSPs to identify the users.

- 2.12 One of the key issues raised in the consultation paper was that of the ownership of personal data. This is arguably one of the more fundamental issues with respect to determining the framework of rights and obligations over personal data. The Authority notes the difference between ‘ownership’ and ‘control’ of data. The former term refers to a proprietary right in a thing or claim, while the latter refers to the competence to take decisions concerning the data.
- 2.13 With regard to ownership of personal data, most of the stakeholders were of the view that the ownership of personal data should ideally be of the individual about whom such data is related and the individual should have the primary rights over such data. Some stakeholders caution about creating a purely property based framework around personal data as data can be replicated infinitely hence it can be infinitely distributed.

Analysis

- 2.14 It must be remembered that identifiability often depends on context. For instance, an IP (Internet Protocol) address or MAC (Media Access Control) address of a device, when seen independently may not qualify as ‘personal data’ but when aggregated along with the Meta-data of the user device or indeed subscriber information, may qualify to be personal data. Hence it is important to consider the context also while classifying a data as “personal data”. The existing legal framework in

India defines the terms "data", "information", "personal information" and "sensitive personal data or information" as under:

- (a) "**Data**" – defined in section 2(1)(o) of the IT Act, 2000 as *a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.*
- (b) "**Information**"– defined in section 2(1)(v) of the IT Act, 2000 as *a term including data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche.*
- (c) "**Personal information**"– defined in the SPDI Rules, 2011 as *any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.*
- (d) "**Sensitive personal data or information**"– defined in the SPDI Rules, 2011 as *such personal information which consists of information relating to:- password, financial information such as bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; biometric information; any detail relating to the above clauses as provided to body corporate for providing service; and any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise; provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as*

sensitive personal data or information for the purposes of these rules.

- 2.15 Personal data has been defined under *Article 4* of the **EU GDPR**⁹ in the following manner:

'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;

- 2.16 As seen from above, the existing definition of personal information/ data under Indian Acts and Rules is in sync with the international trend. Since the definition of personal information/ data would have far reaching implications both in the digital as well as in the physical world, the Authority is of the view that present definitions be continued till the enactment of specific data protection law for the country.
- 2.17 The mode of collection of data may not necessarily effect its classification as the entity capturing the data in physical form may convert the same to binary digital data. Hence the mode of collection of personal data should be irrelevant. The personal data captured by a smart device, camera, microphone, applications etc must be treated in the same manner.
- 2.18 In order to ensure privacy of users, before processing their data, there is merit in ensuring that the same is anonymised/de-identified. However, keeping in view the risks of de-anonymisation/re-identification of users using latest computing techniques by unscrupulous entities for personal gains, the Authority is of the view

⁹ <https://gdpr-info.eu/art-4-gdpr/>

that a technologically neutral approach be taken for anonymisation/de-identification and that on that basis, certain standards for anonymisation/de-identification of data need to be put in place. Since, in certain cases, metadata can be used by the entities operating in the digital eco-system itself to identify the individual users, such entities must be restrained from using metadata to identify the users/individuals.

2.19 In respect of the ownership of personal data, the Authority is of the view that the individual must be the primary right holder qua his/ her data. While the right to privacy should not be treated solely as a property right, it must be recognized that controllers of personal data are mere custodians without any primary rights over the same. For instance, it would appear illogical/ inequitable to permit complete transfer of rights over an individual's personal data. This would imply that, the personal data can no longer be used/ accessed by the data owners – a situation which is quite clearly untenable. In the circumstances, there must be a recognition that while data controllers may indeed collect and process personal data, this must be subject to various conditions and obligations – including importantly, securing explicit consent of the individual, using the personal data only for identified purposes, etc. The entity that has control over personal data would be responsible for compliance with data protection norms.

2.20 **In light of the aforesaid, the Authority recommends:**

- (a) **The definitions of “Data” as provided under Information Technology Act, 2000, and “Personal Information” and “Sensitive Personal Data and information” as provided under Sensitive Personal Data and Information Rules, 2011, as reproduced below, are adequate for the present.**
 - (i) *“Data” – defined in section 2(1)(o) of the Information Technology Act, 2000 as a representation of information, knowledge, facts, concepts or instructions which are being*

prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

- (ii) "**Personal information**" – defined in the Sensitive Personal Data and Information Rules, 2011 as any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.
- (iii) "**Sensitive personal data or Information**" – defined in the Sensitive Personal Data and Information Rules, 2011 as such personal information which consists of information relating to:- password, financial information such as bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; biometric information; any detail relating to the above clauses as provided to body corporate for providing service; and any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise: provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

(b) Each user owns his/ her personal information/ data collected by/ stored with the entities in the digital ecosystem. The entities, controlling and processing such

data, are mere custodians and do not have primary rights over this data.

- (c) A study should be undertaken to formulate the standards for anonymisation/ de-identification of personal data generated and collected in the digital eco-system.**
- (d) All entities in the digital eco-system, which control or process the data, should be restrained from using metadata to identify the individual users.**

B. Sufficiency of existing Data Protection Framework

2.21 Telecom sector is fairly organized and the TSPs are governed by a number of guidelines relating to protection of user data. There are a number of applicable legislation and policies that contain provisions with a bearing on the right to privacy and data security in the telecom sector in India. These include:

- (a) IT Act, 2000: Sec 43A, Sec 69, Sec 69B, Sec 72A, Sec 67C, and Sec 79.
- (b) IT Rules
- (c) Indian Telegraph Act, 1885: Sec 5 and Sec 26,
- (d) Indian Telegraph Rule 419A.
- (e) Unified License condition 37, 38, 39 and 40.
- (f) Guidelines, circulars, direction, and notifications issued by DoT and TRAI

2.22 Under Section 70 of the IT Act, 2000, Telecom Sector has been designated as one of the most important Critical Information Infrastructure by National Critical Information Infrastructure Protection Centre (NCIIPC) as incapacitation or destruction of this sector would result in debilitating impact on the national security, governance, economy and social well-being of the nation. In addition

to the above, in February, 2010, TRAI issued a directive to all TSPs requiring them to ensure compliance of the terms and conditions of the licence regarding confidentiality of information of subscribers and privacy of communications. The Authority had directed the service providers to put in place appropriate mechanisms to prevent the breach of confidentiality of information of subscribers and furnish the details of the steps taken in this regard. The source of generation of unsolicited calls and bulk SMSs may be attributed to unlawful access to consumer's personal information hence it poses a threat to consumer privacy. Unsolicited calls and bulk SMSs can also be used as a tool for phishing attacks. Hence, the National Customer Preference Register (NCPR) was created to protect the privacy of telecom subscribers.

- 2.23 In response to the questions on sufficiency of existing data protection framework and need to bring parity between the OTT service providers and TSPs raised in the CP, most of the TSPs and Telecom Sector Associations were of the view that the provisions included in the UASL related to the privacy of the customers and data protection are sufficient. They were, however, of the view that licensing framework is applicable only to the TSPs while other players in the eco-system like the OTT communication service providers, content providers, device manufacturers, browsers, operating system developers etc. are not covered with similar conditions, leading to a scenario wherein same data is governed by different set of rules in the same ecosystem.
- 2.24 A few stakeholders, comprising of Associations of Application Providers and companies in the software business were however of the view that OTT services are not comparable to the TSPs as the TSPs have an assured revenue business model, they own the infrastructure, and have the primary right over their spectrum. In the absence of assured revenue streams, OTT players have to devise innovative

models for revenue generation without charging the end users for the OTT services that are provided to them.

- 2.25 Some stakeholders from the Software Industry were of the opinion that there is no need to ensure parity as the internet-based services and TSP-services operate in completely different market segments with unique regulatory and economic concerns. Treating them at par would fail to recognize these crucial distinctions and result in inefficient regulation. Further, they submitted that there is no need for introduction of additional data protection requirements to bring parity as the data protection requirements as incorporated in the IT Act, 2000 apply to all the stakeholders in the internet ecosystem.
- 2.26 They further submitted that, TRAI, in the interim may seek information on the specific practices undertaken by TSPs to ensure compliance with Clause 37 of the UASL. Since OTT applications are unlicensed, they do not have to comply with TRAI regulations. They however have to abide by the provisions of the IT Act, 2000 and the complementing Rules. Also, OTT applications should not be subjected to licensing as it will hamper innovation. These stakeholders had also quoted that DoT had rightfully concluded in 2015 that licensing requirements for OTTs were not warranted and TRAI should likewise conclude the same here.
- 2.27 Some stakeholders had submitted that though certain enabling provisions are present in the statute books, the overall framework for data protection of users / telecom subscribers as well as enforcement mechanisms require development. For instance, while the UL requires TSPs to protect the privacy of their customer's data, there are no specific or detailed requirements on issues such as access, correction, data breach, etc.
- 2.28 A large number of respondents were of the view that in order to ensure that an individual's data privacy is protected an independent

statutory authority responsible for data protection should be set up in India under the proposed data protection law. The proposed authority should have jurisdiction over all entities dealing with the data of Indian residents – irrespective of their physical location. The functions of the data protection authority should include:

- (a) Standard setting including through regulations and codes of conduct monitoring and supervision.
- (b) Investigations and enforcement, including through punitive action.
- (c) Grievance redressals to ensure users' rights are effectively protected.
- (d) Coordination with privacy authorities and other relevant entities in other countries
- (e) Making recommendations to the government on issues where intergovernmental action is required in the data privacy field.

2.29 Further, some stakeholders also mentioned that the IT Rules are ambiguous and do not define the roles and responsibilities of data controllers and processors and do not set out clearly the nature of the data that the rules are applicable to. Further, the IT Act provides only a compensation mechanism and does not provide for penalties or consequences for failure to comply with the IT Rules. With regard to data protection issues in the telecom sector, some stakeholders highlighted the following through their submissions:

- (a) There is a need for an overarching principle based privacy law together with relevant enforcement mechanisms to protect the privacy of all Indian citizens.
- (b) It is critical for government to ensure consumer education and awareness.

- (c) Policy makers need to focus on principles, and leave implementation to the industry.
- (d) Regulatory focus needs to shift from ‘operational’ risk management to ‘design’ risk management approach. Concepts like privacy by design within an accountability model are essential. Any standards which are notified may be as per international standards to enable the benefits of standardization

2.30 One of the stakeholders submitted that, the consumers are subjected to complex one-sided user privacy contracts. In many cases, the consent obtained from users is “pre-agreed” or default, and the user has no choice but to accept them. In other cases, the devices come with inbuilt pre-conditions of use which can seriously jeopardize the privacy and security of the users by accessing and transferring user data without his/her knowledge. According to the submission, the existing regulatory framework for data protection suffers from following limitations:

- (a) Limited protection for personal information: The data protection rules under Section 43A of the IT Act,2000 apply only to a narrowly defined category of Sensitive Personal Data and not all forms of personally identifiable data.
- (b) Lack of regulation of the Government sector: Section 43 A of the IT Act, 2000 apply only to Body Corporate and are not extended to Government sector resulting in a lack of data protection standards for collection and use of data by Government sector entities.
- (c) Inadequacy of provisions on privacy policies: Requirements of Privacy Policies need to be strengthened in various respects like notice prior to collection, short and easy to understand terms and conditions of use, notification in case of any change in policies etc.

- (d) Inadequacy of provisions on consent: Consent has been defined to be a onetime mechanism not requiring renewal when modifications are made to privacy policy. Section 43 A does not facilitate easy access and execution of opt out mechanism by the user.
- (e) Limited access and correction protections: Data access for the users is limited to the information provided by them, ignoring present day mechanisms that collect data both directly and indirectly. There also no rules and standards that mandate availability of data to users in a structured, easy to understand format. There are also no provisions which allow the users to edit or move their collected data.
- (f) Broad data retention terms: The purpose and collection limitations under Section 43A are applicable only to Sensitive Personal Data and Information and not to all personal data. The standards fail to connect the consent provided to purpose and duration of retention of data.
- (g) Restrictions on encryption: Certain communication license agreements set out restrictions on encryption. For instance, the Internet Service Provider (ISP) License Agreement requires ISPs to obtain prior governmental approval to deploy encryption which is higher than 40 bits (Part 1, Clause 2(vii)). The Unified License agreement (Clause 37.1), the Unified Access Services License agreement (Clause 39.1), and the ISP license agreement (Part 1, Clause 2(vii)) all prohibit bulk encryption by TSPs.

2.31 The stake holders were of the view that TRAI, being a regulatory authority for telecom services providing internet access only, devising mechanisms to control other stakeholders like content providers and application service providers may be an overreach for the Authority and, perhaps, should be avoided. They were of the opinion that Device manufacturers, service providers, sellers, and all entities involved in

manufacturing, sale and provision of devices and services should not be allowed to interfere with secure data transfers and secure communications. These entities should be held responsible for any data breach due to their systems, software, or otherwise

Analysis

- 2.32 In the absence of a comprehensive data privacy framework, users of the telecommunication/ digital services are subjected to one sided user agreements which are complicated and are difficult to understand. In many cases, these consents are “pre-agreed” and the user has no choice but to accept them. In many cases, the devices come with pre-agreed conditions of use which can seriously jeopardize the privacy and security of the users by accessing and transferring user data without his/her knowledge. User’s data may, therefore, not be protected while stored in the digital eco-system. The need for a more symmetric, all encompassing principles based and horizontally applicable data protection framework for all the players in the digital eco-system is therefore urgent and inescapable. Since the data is collected by private as well as government entities, the data protection framework should be equally applicable to both the Government as well as private entities.
- 2.33 Some categories of data of an individual are protected by the SPDI Rules, 2011. The enforcement / penal provisions provided under the IT Act, 2000 are not stringent enough to ensure protection of individual's personal information/ data. For example, section 43 A of the IT Act,2000 provides for punishments in the event of negligence in securing sensitive personal data, thereby leading to wrongful loss or gain to any person. The maximum penalty payable under Sec 43A of the IT Act,2000 is Rs five crore. Low penalties/ fines may not act as deterrent for the offenders and hence, there is a need to strengthen the existing data protection framework by imposing stringent norms for the entities and penalties for the offenders.

- 2.34 With the rapidly evolving technology, geographical boundaries have been obliterated in the digital ecosystem. Several multinational companies with minimal physical presence/ infrastructure in the country have large consumer base for communication/ digital services. There is a need to protect the rights of such consumers even qua these service providers.
- 2.35 Earlier, the telephone instruments used for establishing the calls and speaking with other side person were non-intelligent in the sense that the processing of data, decision making, and recording of the call details used to take place at the network plane. Due to exponential growth in technology, depending upon the use case, now substantial amount of data processing, decision making, and recording of the call details takes place at the device, browser, operating system and application level also. The devices are being packed with more and more intelligence, computing, and processing capabilities thereby playing an active role in the delivery of services to the consumers and accordingly these have become part of the network. It has enabled delivery of rich consumer experience but has also resulted in higher vulnerabilities to user's privacy and data security. Earlier, the service providers used to maintain users information in the form of call data records, records of access to internet etc but today, users data in the form of browsing history, call logs, location data, contact details etc are captured by the devices, browsers, Operating systems, and Applications also. Since these entities are not governed by the license conditions, applicable for Telecom Service Providers, the need for regulation of these entities of the digital eco-system to ensure protection of consumers' privacy and data security is urgent and inescapable.
- 2.36 Irrespective of whether the application service provider or any other entity in the digital eco-system has level playing field with TSPs or not, security and privacy of the individuals using telecommunication/

digital services, and protection of their personal data is essential. A need, therefore, exists to have uniformly applicable data protection framework for all the entities operating in the digital eco-system.

- 2.37 Existing laws and license conditions governing the TSPs may be sufficient from a broad perspective as they recognize the privacy rights of users. The Authority is of the view that till such time a general data protection law is notified by the government, the existing Rules/License conditions applicable to the Telecom Service Providers for protection of users should be made applicable to all the entities in the digital eco-system. Also, the government should notify the policy framework for regulation of Devices, Operating Systems, Browsers and Applications.
- 2.38 In order to ensure privacy of users, right from inception, data protection framework should be embedded and enforced at each point in the digital ecosystem. To accomplish this objective, adopting "Privacy by design" could be a possible approach. "Privacy by design" refers to the conceptualizing and building of systems with a view to ensuring privacy of users' data. Adoption of Privacy by Design principle implies that appropriate policies, standards, and practices to protect privacy of users must be implemented at every stage where personal data is handled. Further, after obtaining explicit consent of the user, only bare minimum data, which is essential for provisioning of a particular service, should be collected. Collection of unrelated or unnecessary data by service providers in the digital eco-system must be barred. This concept of minimum data collection is referred as "Data Minimisation". This should be an integral part of the "Privacy by Design" concept.

2.39 In view of the above, the Authority recommends:

- (a) The existing framework for protection of the personal information/ data of telecom consumers is not sufficient. To protect telecom consumers against the misuse of their**

personal data by the broad range of data controllers and processors in the digital ecosystem, all entities in the digital ecosystem, which control or process their personal data should be brought under a data protection framework.

- (b) Till such time a general data protection law is notified by the Government, the existing Rules/ License conditions applicable to TSPs for protection of users' privacy be made applicable to all the entities in the digital ecosystem. For this purpose, the Government should notify the policy framework for regulation of Devices, Operating Systems, Browsers, and Applications.**
- (c) Privacy by design principle should be made applicable to all the entities in the digital ecosystem viz, Service providers, Devices, Browsers, Operating Systems, Applications etc. The concept of "Data Minimisation" should be inherent to the Privacy by Design principle implementation. Here "Data Minimisation" denotes the concept of collection of bare minimum data which is essential for providing that particular service to the consumers.**

C. User Empowerment

- 2.40 The Supreme Court in its judgment on 24 August 2017 stated that the “right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 of the Constitution and as a part of the freedoms guaranteed by Part III of the Constitution”. Further, it went on to recognize informational privacy as a facet of the right to privacy and directed the Union Government to put in place a robust data protection regime to ensure protection against the dangers posed to an individual’s privacy by state and non-state actors in the information age.

- 2.41 The epicenter of the entire gamut of Data Ownership, Privacy, and Security revolves around the data consumers (Individuals or Machines). The end user may be more often at a position of low awareness as well as lower bargaining powers when compared to the various entities of the digital ecosystem. This asymmetry is exploited on many occasions by the entities to their advantage. The entities in the digital ecosystem may use personal data of individuals to improve their services; they may even monetize this data by sharing it with third parties. Users often get plagued with bursts of targeted marketing, social media engineering strategies etc not knowing that it was their own data submitted in the past which has enabled such campaigns/strategies. In the absence of necessary data protection framework, the end user does not have any recourse to deal with the exploitation by the entities in the digital ecosystem. Very many times the user is forced to part with his/her personal data with very little information about the scenarios/ uses that his/her personal data would be put to. He has no facilities to access, view, amend, or delete his data submitted. In case of any data breach, he may not even be informed about it till it gets reported. Keeping these concerns in mind, the suggestions of the stakeholders were sought through the CP to empower users so that they can take control of their personal data.
- 2.42 Most of the stakeholders agreed that the existing framework does not provide the requisite wherewithal to the users to protect their personal data in the digital ecosystem. They were of the view that user consent should be mandatory before sharing his/her personal data for commercial/ Non Commercial purposes. Further, the consent should be based upon the category and sensitivity of the information to be collected and the purpose for which the personal information will be used. Some stakeholders submitted that in case of anonymized data and / or data available in the public domain, users consent may not be required.

- 2.43 A large number of respondents had submitted that *notice and consent mechanism* as proposed by the Justice A P Shah Committee¹⁰ needs to be instituted for empowering the end users. They were of the view that the present system of agreement which a user is made to accept is very complicated. Usually, the agreements are lengthy, confusing, one-sided favoring the large data controllers, device manufacturers, application and content providers etc. The end user has no option but to accept these to avail the services. Many a time, if the user declines to agree with these agreements, he/she is denied the services. The users, therefore, do not have any other choice but to accept these agreements. Further, in case of data breach or misuse of his/her personal data, the user is neither informed nor does he/he/she have a mechanism for grievance redressal.
- 2.44 Some stakeholders were of the view that users should have the right to know the purpose for which his/her personal data is being collected by the entity. Users should also have the right to access, view, edit, delete, and move their personal data collected by the entities in the digital eco-system. User should be able to monitor the usage of his personal data by various entities and no third party should be allowed to utilize a user's data without specific permission.
- 2.45 Many stakeholders submitted that there is a need to increase *consumer awareness about* digital privacy principles, user rights, and potential harm in case of breaches or consents given unknowingly. They suggested that every company, entity, digital player be required to place its *Data Protection, Security and Privacy Policy in the public domain/on its website*. The Policy may describe the type of information collected, the purpose of use of the information, to whom or how the information can be disclosed and the reasonable security practices and procedures followed to safeguard the information.

¹⁰ http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

- 2.46 A large number of respondents were of the view that the user should be informed about the duration for which his personal data would be held by the entities collecting/processing this data. Customer should have the right to stop the services along with the right to be forgotten by seeking the deletion of all the information, which an entity/individual has stored previously. The entities should not store and use the personal information of their customers once they stop using the services/products of that entity, beyond the mandated period under the law.
- 2.47 Some stakeholders were of the view that user should have the Right to Opt-in \Opt-out for data. Also, Inter Application data transfer that is compliant with the data protection laws should be enabled. User should be able to move his data on will, from one entity to another seamlessly.
- 2.48 A few stakeholders had submitted that the entities in the eco-system collect personal data from the users even though such data may not be actually required for the functioning of such applications/device.
- 2.49 Additionally, the stake-holders submitted the following measures to empower the end users/data consumers:
- (a) Users should have the right to withdraw their consent for collecting, processing, and sharing of their personal data unconditionally unless it falls under the lawful obligation of the data controller.
 - (b) Every company, entity, digital player be required to place its Data Protection, Security and Privacy Policy in the public domain and on its website. The Policy may describe the type of information collected, the purpose of use of the information, to whom or how the information can be disclosed and the reasonable security practices and procedures followed to safeguard the information.

- (c) Foreign companies establishing their businesses (Content and App services, Device Manufacturing, Browser, OS etc) in India that connects with users through TSPs must ensure that their local entities adhere to the relevant Indian laws governing data privacy and secrecy.
- (d) Data Controllers should not be able to use "pre-ticked boxes" to gain users consent nor imply their consent from other actions.
- (e) Right against unfair denial of service in case he decides not to accept the pre-installed one sided end user agreements furnished by various entities before using their services.
- (f) In case of a data breach whether reported/not reported, it would be mandatory on part of the Data Controller to inform the user about the data breach within 48 hours from the time of occurrence of breach/time of reporting to the user. The Data Controller should also intimate the user about the actions taken to prevent such breaches.

Analysis

2.50 As brought out earlier in the chapter under the sufficiency of the existing data protection framework, the Rights available to the consumers for data protection are limited. The Service Providers, Devices, Browsers, Operating Systems etc have an asymmetric advantage over the end user who is ultimately forced to accept the one-sided agreements/Terms and Conditions to avail the services, equipments etc.

2.51 Notice, Choice, and Consent are the most important rights that should be given to the data Consumers. As per the Justice A P Shah Committee report, Notice means that a data controller, which refers to any organization that determines the purposes and means of processing the personal information of users, shall give simple and easy to understand notice of its information practices to all individuals, in clear and concise language, before any personal

information is collected from them. Such notices should include disclosures on what personal information is being collected; purpose for collection and its use; whether it will be disclosed to third parties; notification in case of data breach, etc. Similarly, Choice and Consent implies that a data controller shall give individuals choices (opt-in/opt-out) with regard to providing their personal information, and take individual consent only after providing notice of its information practices. Consent may be considered to be a powerful means of protecting an individual's information. An individual is best placed to decide the sensitivity of his/her information rather than the Government or any other agency deciding it on his behalf. For meaningful use of these rights by consumers, there is a need to increase consumer awareness about digital privacy principles, user rights, and potential harm in case of breaches or consents given unknowingly.

2.52 The issue of Consent has been addressed by the Government to some extent in the past where in the guiding principles for sharing of user data across services after obtaining user consent have been outlined in the following key policy documents:

- (a) The policy on “Open Application Programming Interfaces (APIs) for the Government of India¹¹” published by MeitY.
- (b) The “National Data Sharing and Accessibility Policy (NDSAP)-2012¹²” by the Department of Science and Technology.

Subsequently, the “Electronic Consent Framework¹³” has been developed by Meity incorporating the guiding principles mentioned in the policy documents mentioned above.

2.53 Subsequent to the development of the Electronic Consent Framework by MeitY, RBI, on behalf of all the Financial Sector Regulators, has

¹¹ http://meity.gov.in/writereaddata/files/Open_APIs_19May2015.pdf

¹² <https://data.gov.in/sites/default/files/NDSAP.pdf>

¹³ <http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf>

issued the master direction known as the "Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016" for all the Financial Sector participants. It has the concept of the data fiduciary (Account aggregator) that, after obtaining the consent of the customers electronically, collects the information from providers of information based on the standardized consent artifact and securely transmits the same to users of the information. This direction is for the benefit of financial sector consumers, as it empowers them to use their personal data, in the form of financial transactions history, for availing new services from any other competing service provider. In light of the same, there is a need to develop a similar consent framework for telecom sector. Once the framework for data privacy and security is approved by the Government, the Authority may work on such framework.

- 2.54 Many times, end user agreements/terms and conditions that a user is served at the time of availing any services, procuring any device etc are one-sided, complex, lengthy, full of legal jargon and in a language that a user may not understand. The user has no other choice but to accept them to avail the services of the entity. Since India is a multi-lingual country, these agreements, notices etc should be provided in an easy to understand, short, multi-lingual format for the benefit of the users.
- 2.55 In order to ensure sufficient choices to the users of digital services, granularities in the consent mechanism have to be built-in by the service providers. User should be able to selectively give his/her consent for each purpose separately rather than a blanket consent for all conditions. Also, the service provider should not deny all the services to user on the pretext that the user has not given blanket consent for all conditions. Any form of implied consent (water-fall model) by the service should also not be permitted. Further, in spite of the users' consent for specific purposes, data controllers as well as

data processors or any other entity handling personal data of the user should be made accountable in case of any unintended harm to the users. Mere accordance of consent by the user to use his/her personal data should not imply that the data controllers, data processors or any other entity in the digital eco-system have been absolved of their responsibilities from any unintended damage caused to the users.

- 2.56 On many occasions the end user of the device is served with one sided pre-stored agreements on these devices after he has bought them. In case the user decides not to agree with these terms of agreement he may not be able to use all the features of the device. Many of such devices are sold with a set of pre-installed applications, which otherwise are not necessary to operate the device. This usually includes a Search Engine, a messaging service, cloud storage, a video service, map services, and browser etc. These Apps in many cases are integrated with the operating system of the device. In case, he agrees to such conditional agreements; the operating system of the device and these pre-installed applications may transfer/upload/utilize the users' data stored/ being used on the device with/without his consent. Simultaneously, if a user wants to share his/ her own data, generated while using the telecommunication/ digital services, with any third party App, the data controller i.e. the operating system of the device or the corresponding application may not allow him/ her to share such data in spite of the fact that the primary right on such data is of the owner of the data. It has also been noted that such pre-installed Applications can neither be deactivated nor deleted. Such situations are detrimental to basic consumer rights and his right to privacy. User should therefore be empowered to delete such pre-installed applications which otherwise are not necessary to operate the device. Deletion of pre-installed applications, which are not part of the basic functionality of the device, should not hamper the functionality of these devices. The user must be free to install/ delete an application at his/her will and the device should in no manner

restrict/disallow the user to do so. Functionality of auto-upload of user data stored on the device should be disabled by default.

- 2.57 Many times, it has been noted that some entities in the digital ecosystem collect personal data of the users even when such data may not be actually required for the functioning of such application/device e.g. for using an application that activates flashlight as a torch on a mobile device, the application seek permission for access to camera, microphone, and contact list etc. The flash light application simply creates a logical circuit between the battery and the camera flash light and does not require access to camera, microphone, or contact list for its operation. It has also been reported that the applications may deploy a waterfall model of consent wherein once an entity is given consent by the user for a particular application or service, the entity translates the consent to many other entities on its own without obtaining explicit consent/knowledge of the user which is a serious breach of users personal data, choice, and consent. Concept of Data Purpose limitation and Collection limitation was proposed by the Justice A P Shah Committee, wherein a data controller shall only collect personal information from data Consumers as is necessary for the purposes identified for such collection. It is, therefore, important that entities in the digital ecosystem should not be allowed to have indirect or inferred consents. It was brought out in paragraph 2.38 that data minimization should be incorporated as an integral part of 'privacy by design' principle. It is reiterated that the concepts of Purpose limitation and Collection limitation have to be enforced rigorously. It has been seen that there is no mechanism by which the user can know about the type of his personal data that is being collected by various entities, the potential use that this data would be put to by the entities, the duration for which this data would be held, the location of personal data, whether the data being sought by the entity is actually required to avail the services, the format in which this data would be stored. The end user neither has access to his

personal data, nor can he edit, delete or move his data at will. In view of the foregoing, the end users have to be empowered by bestowing upon them the rights which can facilitate them in enjoying better data privacy.

- 2.58 On many occasions it has been found that a user is stuck to a particular device, application or service as his personal data cannot be migrated to another device, applications etc. This limitation is exploited by the entities in the eco-system to their advantage. Even if the user discarded the device or unsubscribed services, his personal data continued to be available with the previous device or service provider. The issue can be addressed by implementation of data migration/ data portability policies in the data privacy framework. Related to this issue is the users right to be forgotten, where in it becomes obligatory on the part of the data controller to delete all the information of the data Consumers held with them. Provisions of Right to be forgotten have also been included under **Article 17¹⁴** of the **EU-GDPR**. The right to be forgotten would empower the user to delete past data that he may feel is unimportant or detrimental to his present position. Past data could be in terms of photographs, call records, video clippings etc that may potentially harm the reputation of the data consumers. Since information related to a person may be termed as his personal data and that the user owns such data hence he should be empowered to delete all such data at his discretion. It is also important to note that the "*Right to be Forgotten*" should be implemented with necessary safeguards as there may be requirements by the Law Enforcement Agencies/Licensing conditions etc wherein retention of data in terms of quantum as well duration would be necessary as per applicable legal framework, licensing conditions, hence "*Right to be Forgotten*" should be implemented with applicable restrictions. Further, to address the complaints of users about any misuse of their personal data or regarding violation of the data

¹⁴ <https://gdpr-info.eu/art-17-gdpr/>

protection framework by any entity in the digital ecosystem, a mechanism for grievance redressal should be put in place.

2.59 **In view of the foregoing, the Authority recommends the following:**

- (a) **The Right to Choice, Notice, Consent, Data Portability, and Right to be Forgotten should be conferred upon the telecommunication consumers.**
- (b) **In order to ensure sufficient choices to the users of digital services, granularities in the consent mechanism should be built-in by the service providers.**
- (c) **For the benefit of telecommunication users', a framework, on the basis of the Electronic Consent Framework developed by MeitY and on lines of the master direction for data fiduciary (account aggregator) issued by Reserve Bank of India, should be notified for telecommunication sector also. It should have provisions for revoking the consent, at a later date, by users.**
- (d) **The Right to Data Portability and Right to be Forgotten are restricted rights, and the same should be subjected to applicable restrictions due to prevalent laws in this regard.**
- (e) **Multilingual, easy to understand, unbiased, short templates of agreements/ terms and conditions be made mandatory for all the entities in the digital eco-system for the benefit of consumers.**
- (f) **Data Controllers should be prohibited from using “pre-ticked boxes” to gain users consent. Clauses for data collection and purpose limitation should be incorporated in the agreements.**
- (g) **Devices should disclose the terms and conditions of use in advance, before sale of the device.**

- (h) It should be made mandatory for the devices to incorporate provisions so that user can delete such pre-installed applications, which are not part of the basic functionality of the device, if he/she so decides. Also, the user should be able to download the certified applications at his/ her own will and the devices should in no manner restrict such actions by the users.
- (i) Consumer awareness programs be undertaken to spread awareness about data protection and privacy issues so that the users can take well informed decisions about their personal data.
- (j) The Government should put in place a mechanism for redressal of telecommunication consumers' grievances relating to data ownership, protection, and privacy.

D. Rights and Responsibilities of Data Controllers

- 2.60 Data Controllers are those entities in the digital eco-system who, either alone or with others, determine the purposes and means of processing of personal data. Control refers to the competence to take decisions about the contents and use of data.¹⁵ The entity that controls the data i.e. determines the purposes of processing, the means of processing, the sharing of data etc., should be primarily responsible for the compliance with data protection requirements. Data processors on the other hand are those entities who process data on behalf of data controllers.
- 2.61 In practice Data Controllers can be providers of Devices, Operating Systems, Applications, Web Browsers, Service Providers etc. as they collect, store, and control telecommunication consumers personal data.

¹⁵ Available at
<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowofpersonaldata.htm#part1>.

- 2.62 As discussed in the previous sections, users in India have limited rights to access, edit, or delete personal data held by various entities. The recent instances of data breaches/data thefts in the world demonstrate the tremendous power that data controllers and processors can have – insofar as data analytics has purportedly been used to influence voter behavior in different countries. At the same time, it is also worthwhile to note that data is required for creating and driving new businesses and innovation, and further that unnecessary or excessive regulatory costs on data driven businesses may only hamper growth of the sector.
- 2.63 Keeping in mind the balance required to be struck between the rights of data consumers and the need to encourage data driven businesses, the Authority posed a question concerning the rights and responsibilities of data controllers in the digital ecosystem.
- 2.64 In response to the question, a majority of the stakeholders were of the view that the rights of the data controllers cannot supersede the rights of the data consumers over his personal data. A few respondents submitted that the rights and responsibilities of data controllers should be similar to other entities of the ecosystem while some others had proposed that separate sectoral guidelines may be proposed for data controllers of each sector.
- 2.65 Many stakeholders were of the view that a data controller should collect, process, disclose, make available, or otherwise use personal information only for the purposes as stated in the notice after taking consent of individuals. If there is a change of purpose, this must be notified to the individual, and only after the individual has consented to the new purpose, should the data be processed for such purposes.
- 2.66 One respondent submitted that there needs to be clear reporting requirements for data controllers to publish periodic transparency reports. These reports should include information about data processing practices for better information of users. Further, the

reports should also highlight any security incidents and steps taken by the data controllers to address the issues. Accordingly, the policies prohibiting disclosures about interception, monitoring, and decryption need to be modified.

- 2.67 Some stakeholders had opined that responsibilities for data controllers should include adherence to and expert knowledge of all applicable data protection laws, regulations and practices affecting the organization in question. In addition, data controllers must always maintain a direct reporting access to the highest level(s) of an organization; issues like information and data security are enterprise-level concerns, and those responsible for their safeguarding should liaise directly with the decision makers at the pinnacle of the organization. Creating a Data Control Authority (possibly as a division of a proposed Data Protection Authority) as a mechanism for governing, regulating and educating data controllers is strongly recommended. Centralizing these functions would enable better information dissemination to all involved.
- 2.68 Many respondents were of the view that regulatory principles are required to be defined for the data controllers, data processors etc by the government. Once defined, a centralized Data Protection Authority should regulate and enforce the framework on all the stakeholders.
- 2.69 Some stakeholders had submitted that it was best left to the industry to self regulate the data controllers by having in-house industry best practices to govern and regulate. The data controllers would be ranked by the industry itself based on their performances and the best practices followed by the data controllers.
- 2.70 Some stakeholders have proposed the following responsibilities of the data controller:
 - (a) Data controllers must be held responsible for ensuring the security of personal and sensitive personal data. There should be

an oversight mechanism for Rule 8 of the SPDI Rules, to ensure that data controllers are taking enough measures to protect the data.

- (b) Data controllers must give notice of data breaches to CERT-in, sectoral regulators and affected data consumers.
- (c) Data controllers must notify data consumers about what data will be collected, for what purpose, by whom, who to contact in case of grievance, what would be the effect of agreeing to or disagreeing to the collection of any data. Such notices should be simple and easy to understand, and must be available in English as well as the vernacular language of the region in which the data controller is providing their services.
- (d) Data controllers must ensure that anyone with whom personal information or sensitive personal data or information is shared obeys the same standards of security and privacy as are applicable on the data controller. The transfer of data should not be allowed without explicit consent from the data consumers. Transfer of data must not be allowed to another country unless the country to which the data is being transferred offers similar levels of protection to personal and sensitive personal data.
- (e) Personal data must not be published openly. Any exceptions such as for journalism, research, household use etc., must be narrowly defined. Broad exceptions would serve as a source of exploitation.
- (f) Any collection, use, storage or transfer of personal data must not be done without prior explicit informed consent from the data consumers.
- (g) Data controllers must be transparent about their security procedures and practices, and data collection, use and transfer policies and these should be published in the form of a privacy policy.
- (h) Data controllers must train their staff in security procedures.

- (i) Data controllers must ensure that access to personal and sensitive personal data is restricted to only those people who must necessarily have access to it in order to perform their duties. In all other instances, such data must be out of reach for employees and outsiders.

Analysis

- 2.71 Currently, the term "data controller" is not defined in any legislation or regulation in India. The IT Act utilizes the term 'Body corporate' which limits the application of extant privacy law (for instance by excluding certain government agencies such as Ministries and Departments). There is, therefore, an urgent need for defining the concept of data controllers and data processors in a comprehensive manner, keeping in view the variety of entities who may gather and process personal data of individuals. Thereafter, the privacy framework may lay out relevant obligations and practices that should be observed by all such entities.
- 2.72 Segregation of entities into data controllers and data processors is useful in apportioning responsibilities on the various parties involved in dealing with personal data in the digital ecosystem. Often, entities will merely collect and pass on personal data to external entities for further analysis. It is therefore necessary to ensure privacy protections of individuals from all entities in the digital ecosystem.
- 2.73 Since data controllers collect and store users' data; they gain unhindered access to such data which can be put to use by them at their discretion. The user has no control over this data in the absence of any regulatory framework. Hence, the scope of powers that data controllers have should be strictly limited by the nature of consent provided to the data consumers or as otherwise required in the law.
- 2.74 One of the first steps in ensuring adequate privacy protection for users is to provide meaningful choice and ensure appropriate

information is provided to users about the privacy practices and policies of data controllers. Accordingly, appropriate responsibilities and obligations must be placed on data controllers to ensure proper notice regimes are implemented, there is transparency about information practices, users are empowered through data portability mechanisms, informed of data breaches, provided adequate remedies, etc. In addition, it should be incumbent on data controllers and processors to implement appropriate security measures, privacy by design principles, etc. The “Principle of Accountability” should be made applicable to the data controllers as well as processors so that they can be held accountable for any unintended use or misuse of data.

- 2.75 In addition, it is important to recognise that ownership rights of the individual/user over his/her personal data are supreme and should normally not be superseded by the rights of data controllers, data processors, or any other entity in the eco-system. This necessarily implies that appropriate systems of transparency and accountability must be implemented by all data controllers and processors. This should include internal systems of grievance redress as well as institutional systems of enforcement.
- 2.76 The rights and responsibilities of Data Controllers and Data Processors have to be similar for all sectors of the economy. Accordingly, such rights and responsibilities of Data Controllers and Data Processors may become part of the Data Protection Framework being developed by the Experts Committee under Justice B. N. Srikrishna. Therefore, the Authority at this juncture has decided not to make any recommendations on the Rights and Responsibilities of Data Controllers. However, the Authority may revisit this issue later on.

E. Technology Enabled Architecture to audit use of Personal Data and monitor the Digital Ecosystem.

- 2.77 Enforcement of the Data protection framework requires that Complaint Registration, Investigation, Auditing, Imposition of Penalties, and grievance redressal mechanisms to be in place. Audit is required to ascertain the compliance of systems, policies, and practices by an entity with the data protection framework.
- 2.78 With the development of newer technologies, the degree of sophistication, and speed of data thefts are growing day by day. Due to voluminous data on the internet, it becomes very difficult to monitor compliances and carryout real time audit. Moreover, automated audit mechanism would require deep packet inspection of every data packet moving on the internet; which may in itself tantamount to intrusion in privacy of the data consumers.
- 2.79 The entities in the digital eco-system are increasing exponentially. Further, the situation would become alarming when viewed with the number of M2M devices in near future. The personal data collected by the data controllers and processed by the data processors would be in several Zetta Bytes. Hence, it would be humanly impossible to monitor the entire eco-system to check incidents of data breach or data misuse. Enforcement of data protection framework would therefore not be possible in the absence of a robust Audit framework.
- 2.80 The Authority, having realized the criticality of the issue, had raised questions in the CP and views of the stakeholders on the necessity to establish technology enabled architecture to audit use of personal data and monitor the digital ecosystem were sought. Further, stakeholders were also required to comment on the efficacy of establishing of such a system by the government.
- 2.81 In response to the question on technology enabled architecture to audit use of personal data and monitor the digital eco-system, some

stakeholders submitted that though audits are important but they have limited utility, as they can only look at aspects of procedural compliance and need to be complemented with robust mechanisms for redressal and comprehensive policy. Adoption of a technical framework without adequate development of a rights based data protection framework may not provide any solution for data security or individual privacy. Further, an automated audit system would by itself lead to data centralization and pose risks to users. There would be further problems in its implementation as it would in a sense be a universal backdoor to all internet applications and services. Hence, without adequate security such a compliance system by itself may pose as a security risk.

2.82 Some stakeholders submitted that creation of technology enabled audit architecture is not recommended due to following reasons:

- (a) Higher compliance costs.
- (b) Frequent obsolescence of technology.
- (c) Differences in business models, products/services, data collection practices, and the complexity of algorithms of various entities in the digital ecosystem.
- (d) It may create geo-fences for cross-border businesses.

In view of the forgoing the stakeholders recommended that self-regulation coupled with internal and third party external audits. Further, they said that format, structure, periodicity of certifications may be worked out in consultation with stakeholders. They were of the view that all players in the eco-system be subjected to these audits.

2.83 One respondent submitted that there are limitations to an audit based system in which users have little recourse or remedy. A mix of proactive reporting requirements such as transparency reports and

data breach notification requirements, enforcement and adjudication forums are some of the measures which may safeguard user interest.

- 2.84 Few TSPs were of the view that TSPs already have well established, adequate mechanism for users' data protection and there is no need for creation of technology based audit mechanism as technology alone cannot do the entire audit, human intervention would be required.
- 2.85 Some stake-holders, however, supported the concept to create a technology-enabled architecture to audit the use of personal data and associated consent. Such a mechanism would not only benefit the government but also protect the data consumers. Some stakeholders submitted that a central register containing information for each data controller should be created.
- 2.86 Some respondents submitted that human intervention with support of technology based audit architecture (for checking and keeping track of the consent logs) will help in compliance monitoring and assessment by the entities for e.g., a "fair processing notice" is expressed in a myriad of different ways and contexts, so it is hard for a computer to understand whether the notice is sufficient. In such cases, best practice is for the companies to document their policies and processes and adopt principles that increase accountability. The compliance can be self-assessed by these entities or by accredited standard bodies like ISO for security; or by auditing firms that have the requisite expertise and capability.

Analysis

- 2.87 Audit is an important facet for enforcement of data privacy framework. The Audit framework should not be restrictive yet at the same time it should be adequate to protect the interests of the stakeholders in the ecosystem.
- 2.88 In India, the internet proliferation as well as the consumer awareness is less when compared with developed nations. As brought out earlier,

existing legal framework available in India to address the data privacy issues is in-adequate.

- 2.89 A purely human/manual audit approach may not be advisable due to the magnitude of data being handled, complexities of the technologies at each level, and the need for real time audit of the systems. Moreover, the technology changes occur at a very rapid pace and it would be virtually impossible for the pool of auditors to keep in sync with these changes.
- 2.90 Complete Technology based audit mechanism may also have challenges due to algorithmic biases, justified interpretation of laws by machines may not be possible e.g., a “fair processing notice” is expressed in a myriad of different ways and contexts, so it is hard for a computer to understand whether the notice is sufficient or not.
- 2.91 A hybrid approach with a combination of Technology and the human intervention may be more suited to our context. In case of EU GDPR, it can be seen that a hybrid approach to Audit mechanism has been adopted (Ref Article 28¹⁶,39¹⁷,47¹⁸ and 58¹⁹ of EU GDPR).
- 2.92 The issue of technology enabled audit and monitoring of the digital ecosystem is complex and would have to be derived based on the overall data privacy framework of the country. Primarily, such monitoring and audits would be applicable for data controllers and data processors. As discussed earlier, issues relating to rights and responsibilities of the data controllers may be revisited later-on after the Data Protection Law would be in place. In view of the foregoing, the Authority has decided not to make any recommendations on this issue at this stage. Once the data privacy laws for the country are enacted, the Authority may, if necessary, revisit the issue.

¹⁶ <https://gdpr-info.eu/art-28-gdpr/>

¹⁷ <https://gdpr-info.eu/art-39-gdpr/>

¹⁸ <https://gdpr-info.eu/art-47-gdpr/>

¹⁹ <https://gdpr-info.eu/art-58-gdpr/>

F. Security of Data and Telecom Networks.

- 2.93 Telecom networks may be viewed as carriers of voluminous data traffic between the entities of the digital eco-system. The need to ensure security and privacy of data being carried on these networks as well as the security of the telecommunication networks are therefore of paramount importance. TPSs may also qualify as Data Controllers as they capture large amount of users' data in the form of call logs, browsing history, personal details etc. Since data controllers are responsible for the security and privacy of consumers data, it is important to examine the various provisions under the regulatory framework applicable to the TSPs to ascertain whether adequate measures exists to ensure the security of telecom networks as well as the traffic which these networks carry.
- 2.94 Against this background, the Authority raised the questions pertaining to the measures required to ensure safety and security of telecom networks in the CP.
- 2.95 The TSPs were of the opinion that the existing regulatory framework for the security of telecom networks is adequate. However, some of them felt that use of mandatory 40 bit encryption keys for securing the data on telecom networks was outdated and there was a need to re-examine the basic encryption standards applicable to the TSPs. One of the TSPs recommended the creation of a platform for all the TSPs to share amongst themselves the vulnerabilities and information about the breach incidents to initiate proactive strategies to deal with such eventualities.
- 2.96 One of the stakeholders submitted that following additional steps need to be taken to ensure the security of telecom infrastructure and the digital ecosystem as a whole:
- (a) Companies should have in place and disclose information about their process for responding to data breaches, and must publish

- periodic reports about any security incidents and how they have been responded to.
- (b) All user communications should be encrypted and this should be enabled by default.
 - (c) Companies should regularly publish educational material on security for users.
- 2.97 One of the stakeholders was of the view that information related to various incidents - network threats, breaches, malware, DOS attacks, etc must be shared proactively with the relevant players in the ecosystem and telecom subscribers, in a time-bound manner to reduce potential damage.
- 2.98 Some respondents submitted that one of the preferred approaches could be to encourage the White-Hat community to constantly monitor and proactively report possible threats to the appropriate authority. Use of bug-bounty programs may be encouraged, community building and other such measures may be adopted to build a large base of volunteers/professionals who ensure that the security of critical systems is up-to-date.

Analysis

- 2.99 Since the TSPs are licensed entities in the digital ecosystem, they are governed not only by the License conditions and sector specific laws but they are also required to adhere to several other laws. Some of the important security conditions and standards applicable to TSPs are listed below:-
- (a) Adoption of ISO27001 or sectoral-standard
(Sec 43 A, IT Act,2000);
 - (b) For Network elements: ISO/IEC 15408 (**UL Condition 39.6**);
 - (c) For Management: ISO 27000 (**UL Condition 39.7**),
 - (d) 3GPP2 security standards: (**UL Condition 39.7**).

- (e) Certification : (***UL Condition 39.7***)
- (f) Incorporation of contemporary security standards: (***UL Condition 39.8***).
- (g) Technical Scrutiny and Inspection: (***UL Condition 39.2***)
- (h) Facilities for monitoring of all intrusions, attacks and frauds: (***UL Condition 39.10***)
- (i) Facilities for monitoring by designated security agencies: (***UL Condition 39.12***)
- (j) Organizational security policy, management, network forensics, hardening, penetration test, risk assessment: (***UL Condition 39.5***)
- (k) Maintaining records of software details etc: (***UL Condition 39.9***).
- (l) Adequate and timely measures to ensure that the information transacted through a network by the subscribers is secure and protected. (***UL Condition 39.23(iv)***)
- (m) Data Localization of traffic: (***UL Condition 39.23(iii)***)

In view of the foregoing, it may be inferred that the TSPs have a fairly robust regulatory framework for ensuring the data privacy and security of its consumers.

2.100 Encryption is an important aspect for ensuring the safety and security of the content. In case of the TSPs, use of bulk encryption as well as deployment of high order encryption standards has been prohibited. Since the TSPs provide connectivity to various entities in the ecosystem, the robustness/ strength of the data protection is dependent upon the encryption standards used by each entity. Presently, non-uniform encryption standards are being followed by

various sector regulators. Encryption standards stipulated by various sector regulators are as follows:

- (a) SEBI²⁰- Guidelines on Internet Trading: 64 / 128 bit encryption.
- (b) RBI²¹- Guidelines on Internet Banking: Minimum SSL / 128 bit encryption.
- (c) UIDAI - AADHAAR authentication API specification -Version 2.5²²: Personal Identity Data (PID) block, data should be encrypted with a dynamic session key using AES-256 symmetric algorithm (AES/GCM/No Padding). Session key, in turn, is encrypted with 2048-bit UIDAI public key using asymmetric algorithm (RSA/ECB/PKCS1Padding)
- (d) DoT: Mandates evaluation and approval of encryption equipment, Prohibits bulk encryption and mandates use of maximum 40 bit Key length for encryption. For higher level encryption, DoT mandates seeking of written permission and deposit of decryption keys with them.

Robustness of the user's data privacy and data protection in the digital ecosystem depends upon the weakest link in the ecosystem. Different sectors are following different encryption standards, hence there is a need for harmonization of Encryption standards across the sectors in our country. Accordingly, the Government should notify the National Policy for Encryption of personal data, generated and collected in the digital eco-system.

2.101 For ensuring the end-to-end security of the personal data, its encryption during the motion as well as during the storage in the digital ecosystem is necessary. Decryption could be permitted on a

²⁰ https://www.sebi.gov.in/sebi_data/commondocs/anncir2_p.pdf

²¹ <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/21569.pdf>

²² https://uidai.gov.in/images/resource/aadhaar_authentication_api_2_5.pdf

needs basis by authorized entities pursuant to consent or as per requirement of the law.

2.102 In case of breaches, data thefts etc timely sharing of information with the data consumer and various entities in the digital ecosystem is essential to mitigate the losses/ breaches and prevent their future occurrences. It has been seen that a system of rewards/incentives for compliance and penalties for willful defaulters works best. Hence, a system of voluntary disclosure of information between the entities should be created and incentives/rewards should be given to the service provider/entity giving advance information about any cyber threat/incident. A platform for sharing of such real-time information should be created and it should be made mandatory for all the service providers to be a part of this platform. Active sharing of information about possible threats and vulnerabilities among the service providers would facilitate plugging of gaps in the existing systems, evolution of best practices and voluntary sharing of information. This in turn would result in creating a safe and secure telecom network.

2.103 **In view of the foregoing, the Authority recommends that:**

- (a) Department of Telecommunication should re-examine the encryption standards, stipulated in the license conditions for the TSPs, to align them with the requirements of other sectors.**
- (b) To ensure the privacy of users, National Policy for Encryption of personal data, generated and collected in the digital eco-system, should be notified by the Government at the earliest.**
- (c) For ensuring the security of the personal data and privacy of telecommunication consumers, personal data of telecommunication consumers should be encrypted during the motion as well as during the storage in the digital**

ecosystem. Decryption should be permitted on a need basis by authorized entities in accordance to consent of the consumer or as per requirement of the law.

- (d) All entities in the digital ecosystem including Telecom Service Providers should be encouraged to share the information relating to vulnerabilities, threats etc in the digital ecosystem/ networks to mitigate the losses and prevent recurrence of such events.
- (e) All entities in the digital ecosystem including Telecom Service Providers should transparently disclose the information about the privacy breaches on their websites along with the actions taken for mitigation, and preventing such breaches in future.
- (f) A common platform should be created for sharing of information relating to data security breach incidences by all entities in the digital ecosystem including Telecom service providers. It should be made mandatory for all entities in the digital ecosystem including telecom service providers to be a part of this platform.
- (g) Data security breaches may take place in-spite of adoption of best practices/ necessary measures taken by the data controllers and processors. Sharing of information concerning to data security breaches should be encouraged and incentivized to prevent/ mitigate such occurrences in future.

G. Measures to encourage creation of new data based businesses.

2.104 Data Analytics is an important emerging area that may transform the delivery of services and products in future. It may have immense societal and economic benefits. Data Analytics may be useful in solving several issues like the traffic congestion, disaster

management, supply chain management, etc. It may also facilitate targeted product delivery system, better health care management, personalized education to students, better policy formulation, better law enforcement etc.

2.105 The most fundamental commodity required to operate a data based business is the data itself. Making available large amount of data that is being generated by the individuals or the machines in the ecosystem without any safeguards may not be advisable as it may lead to compromising the privacy and security of the users data. It may also tantamount to the violation of users privacy rights. While it is important to safeguard the interests of the users, it is also important to ensure that new products and services are introduced for the betterment of the society. In view of the foregoing, the Authority sought the views of the stakeholders on the measures that may be adopted to encourage the data based businesses in our country.

2.106 In response, many stakeholders were of the view that public policy focus should be on providing regulatory certainty and consistency, preventing harm to users, preventing misuse of Personal Information/Personal data of the users and making companies accountable through self-regulation. Further, they felt that Government should focus on building an adequate implementation ecosystem, including institutional capacities and capabilities, effective grievance redressal system, user awareness, active civil society, and impetus to research and development. They also submitted that the regulatory framework should be applicable uniformly to all the players in the ecosystem. Some respondents suggested following measures to achieve the creation of new data based businesses :-

- (a) Anonimization of data sets.
- (b) Enabling Data Portability.
- (c) Creation of public data sets.
- (d) Encouraging business related to compliance and data security.

2.107 Some stakeholders were against the data driven businesses and submitted that there should be no relaxation in rules or regulations in order to promote new businesses monetizing users data.

2.108 Few stakeholders representing the software industry were of the opinion that over-regulating the market can interfere with the freedom of trade and dis-incentivize competition, investment, trade, and create business inefficiencies. The government's role should be only of a catalyst and it should create a favorable environment for doing business.

2.109 Some TSPs have submitted that to encourage data driven businesses, the government should implement programs and implement measures that increases consumer awareness and helps in building trust of individuals whose data is being collected by various entities.

2.110 One respondent had submitted that there should not be any relaxation in the rules or any prejudiced application of regulations in order to promote new businesses monetizing data, as it may lead to compromising the privacy and security of user's data.

Analysis

2.111 Data Analytics industry may be considered as a new growth engine of the future as it would be instrumental in solving many modern day issues^{23,24}. Some of the attributes of Data Analytics business are that it is technology intensive, rapidly evolving, high investment in R&D, requires specialist work-force etc. World over, entrepreneurs, MNCs, Governments etc have realized the importance and the capability of Data Analytics and significant efforts are being made to develop this industry.

²³ <http://asiandatascience.com/wp-content/uploads/2017/11/eBook-Big-Data-2017-Market-Statistics-Use-Cases-and-Trends.pdf>

²⁴ <https://wikibon.com/executive-summary-big-data-vendor-revenue-and-market-forecast-2011-2026/>

2.112 Being a large country with a young and upwardly mobile population, India offers a unique opportunity to the entrepreneurs to service the large consumer base. Government may also use data-analytics for the larger good of the citizens. For the people/consumers to share their valuable personal data with the entities in the ecosystem, it is important that the consumers have confidence and trust in the agencies collecting their data. The trust and confidence can be built by having in place a robust data protection framework for the country.

2.113 Data Analytics may act as a force-multiplier in development of our country due to its multi-dimensional benefits. The government is sanguine with the importance of the issue, however equally important is the issue related to data privacy of its citizens. Government has constituted an Experts Committee under Justice B N Srikrishna who are developing the data privacy framework for the country hence the Authority has decided not to give any recommendations at this juncture on this issue.

H. Data Sand-Box

2.114 A Data Sand Box may be visualized as an entity that anonymises data sets which can be utilized by the service providers/ businesses to design new products and services for the benefit of customers and growth of their businesses.

2.115 The Authority, with a view to understand the need, mechanisms, controls, access, and the entities who should be made responsible to establish data sandboxes, raised the question in the CP.

2.116 In response to the question most of the respondents were of the view that Govt. or its authorized authority shouldn't set up a data sandbox that may allow regulated companies to create anonymous data sets due to following reasons:

- (a) It may create roadblock to emerging dynamic business models by chocking investments and innovation incentives.
- (b) Aggregation of information in the form of freely available data sets may lead to higher vulnerabilities.
- (c) Govt has limited incentives in investing in cutting edge technologies.
- (d) It would result in violation of Article 300A of the constitution which prohibits the state from depriving someone of their private property except through statutory law.
- (e) It would be difficult to implement concepts of notice, choice, consent, purpose limitation, collection limitation, or right to object in a data sandbox.

Further, they submitted that sharing of anonymized data between the entities can be preferably based on mutual contracts.

2.117 Some respondents were of the view that the Government may set up a data sandbox only if entities can participate on a voluntary basis and only if the data that is shared on such a data sandbox is raw data and not processed or analyzed data. Further, datasets should be anonymised to ensure privacy of users personal information.

2.118 Few stakeholders had submitted that government should continue to promote publication of data by government agencies under the open data policy. The regulators and government have a significant amount of data that can be anonymised and included in the open data sandbox that would improve transparency and help in development of newer services.

2.119 Some respondents had submitted that establishment of data sandboxes may benefit the consumers as well as the businesses. The consumers would get access to better services and products while the

businesses would be able to generate revenues by offering these services and products to the consumers.

2.120 One of the respondent was of the view that Re-profiling from anonymised data is possible and hence anonymisation may not help in data protection. Further, the respondent cited two research reports, one from the University of Texas²⁵ and the other from the Colorado Law Legal Studies Research²⁶ which showed the possibility of re-identification of users from the anonymised data sets. Since possibilities of re-identification exist, Re-Identifying, De-Identifying data should be treated as an offence.

Analysis

2.121 Development of Goods and services undergo several iterations and testing before they are launched commercially, this may be necessary to ascertain their operational and commercial viability by the consumers as well as the service providers/ manufacturers. With the modern day technologies, it may be possible to create more robust and efficient algorithms that can be utilized to create better services and products. Testing of algorithms on data sets before production of goods/services may be a cost effective methodology since the testing can be carried out on computers with minimal resources.

2.122 Anonymised data sets carved out of existing personal data held with various entities in the digital eco-system for testing the algorithms may be a dangerous proposition due to possibilities of Re-profiling/ Re-Identification of the users²⁷. As mentioned earlier, suitable standards for de-identification/annonymisation would have to be

²⁵ Narayanan, A. and Shmatikov, V, Robust De-anonymization of Large Sparse Datasets, available at https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf

²⁶ Ohm, Paul, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (August 13, 2009). UCLA Law Review, Vol. 57, p. 1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12. Available at SSRN: <https://ssrn.com/abstract=1450006>

²⁷ 5 Nate Anderson, “Anonymized” data really isn’t—and here’s why not, available at <https://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/>

arrived at before permitting use of de-identified/annonymised data sets for the data sand boxes.

2.123 Government, has been publishing open data sets of its various Ministries regularly on their websites, and, in a way, it does provide data sets to the industry/service providers. However, mandatory sharing of data by all the entities with the government and establishing of data sandbox by the government would entail substantial investment in IT infrastructure like data centres, storage farms, power etc on the part of government. Presently the data protection framework for the country is under development. Moreover, the issue of data sand box would require further deliberations post implementation of the data privacy law for the country. In view of the foregoing, the Authority has decided not to make any recommendations related to data sand box at this juncture.

I. Legitimate exceptions to privacy regulation

2.124 The Authority has previously noted the importance of putting in place adequate privacy protections to protect the personal data of users. However, as noted by the Supreme Court in the Puttuswamy case, privacy is not an absolute right and must be balanced, based on the context, with other rights and obligations - for instance the duty of the state to ensure territorial integrity and security of citizens. Accordingly, it is essential that well tailored exceptions are crafted for any privacy policy permitting *inter alia* exceptions for law enforcement, for purposes of research, and so forth. Any exceptions must however be necessary and proportionate - implying that they must be narrowly tailored to meet specific and legitimate requirements. Further, appropriate systems of checks and balances must be introduced to ensure that the balance between privacy rights and the exceptions thereto are appropriately maintained.

2.125 The Authority therefore requested inputs from stakeholders on the legitimate exceptions to the application of data privacy framework and

the checks and balances that need to be instituted to meet the legitimate requirements of the law enforcement agencies.

2.126 In response to the question raised in the CP, most of the stakeholders were of the view that exceptions to the application of data protection framework should include the following:

- (a) Issues when there is a threat to national security and territorial integrity;
- (b) To maintain public order;
- (c) Investigations of crime by law enforcement agencies (LEAs).

2.127 Some stakeholders were of the view that TSPs are governed by a licensing framework which puts them under obligation to provide LEAs with personal data of users (for instance, call data records and location). They further submitted that Over-The-Top (OTT) service providers are under no corresponding obligations to provide such data to LEAs. These stakeholders argue that all entities in the digital ecosystem that provide similar services should be subject to the same regulatory requirements.

2.128 Some TSPs submitted that they should be provided with a legal process to challenge requests by the LEAs when they believe that requests for data may exceed the LEAs authority or are otherwise deficient in some manner.

2.129 One stakeholder submitted that the existing data access requests system is governed by the IT Act and the Indian Telegraph Act, 1885. Both the statutes provide varying standards and procedures for interception thereby creating differences in the interception regimes. These differences have led to creation of an ambiguous regulatory regime which is prone to misuse. Further the stakeholder cited the recommendations of Justice A P Shah committee which proposed harmonization of the interception regime in India and inter alia

suggested that each relevant legislation be amended to comply with the National Privacy Principles. This stakeholder recommended that any data protection law should clearly establish the circumstances under which Government authorities may issue demands for personal information and further there must be a requirement for judicial interventions and oversight over such activities.

2.130 A few respondents submitted that companies should be permitted to report publicly on the number of demands that they receive for personal information on a periodic basis, in order to increase transparency and to inform public debate about the relevant laws.

Analysis

2.131 When it comes to the issue of legitimate exceptions to the privacy regime concerning TSPs, there are primarily three issues at hand:-

- (a) Exceptions concerning requests by law enforcement agencies and /or as may be required under law,
- (b) Exceptions for purposes of carrying out research and statistical analysis,
- (c) Exceptions for the purpose of ensuring optimum quality of services.

It was pointed out by the Supreme Court of India in the Puttuswamy case, all exceptions in addition to meeting a legitimate aim, must be necessary and proportionate. Hence the same principles must be applied to carving out exceptions for TSPs.

2.132 The data privacy framework for the country is under development, and the exceptions to the privacy can be mandated under law only. In view of the foregoing the Authority has decided not to make any recommendations in respect of legitimate exceptions to the Privacy regulatory framework.

J. Cross Border Data Flow

2.133 Data is the new oil for growth in the world today. The need to remain connected 24 X 7 through various modes of communication implies the need for data flow across the geographical boundaries. Businesses in their aspiration to provide better services to the clients and to enhance their global footprint tend to establish their offices, datacenters, logistic facilities etc across the globe. This results in cross border flow of data which includes personal data of customers, business data, employee data etc. The global enterprises in their bid to overcome catastrophic failures due to natural/ manmade disasters, establish Business Continuity Systems at diverse locations to store data pertaining to customers, employees and businesses.

2.134 India, being a software giant and a growing economy has been benefited due to its services business like the BPOs (Business Promotion Offices). Considering the importance of this issue, in the CP, the Authority had sought stakeholder's view on it.

2.135 In response, some stakeholders were of the view that regulator should refrain from making prescriptive policy guidelines that restrict cross border data flow and mandate localization. Cross border data transfer should in turn be regulated not restricted to fully harness the benefits of cloud computing. Geographical mandates may be construed as significant trade barriers and will have negative consequences as there will be possibilities of other countries also start imposing such restrictions which will severely impact the export market. Also, hosting a platform in every country would lead to inferior QoS as the interplay of many platforms cause issues in many aspects and very high costs for the service providers which will discourage investments. Moreover, navigating the data regulation and policy rules across borders can slow implementation of a valuable solution and delay innovation. The restrictions may hamper India firms to overcome in

order to compete in the global economy. The stakeholders opined that it should be user's choice where to keep their data.

2.136 The stakeholders further stated that regulatory requirements can be fulfilled by imposing guidelines on organizations to use good security standards and to check and enforce those standards on behalf of their consumers. In instances where companies are storing particularly sensitive data, they can determine additional security measures, including where data is stored, at the contract level.

2.137 One stakeholder expressed that some of the concerns about cross border data transfer relate to national security can be mitigated through:

- (a) Formulating a list of countries that provide adequate protection of personal data and restricting personal data transfer only to countries on the list
- (b) Enforcing use of modal contractual clauses to regulate transfer of data (as it had been done in the EU)
- (c) Enforcing approved binding corporate rules where transfer is conducted within the same group of entities which are located in different jurisdictions
- (d) Achieving mutual understanding with the relevant regulators within the foreign jurisdiction on the facilitation of cross border transfer (such as the US-EU Privacy Shield that is currently being developed).

2.138 According to some stakeholders, instead of restricting cross border data flow, there is a need to develop mechanisms for cooperating informally or, alternatively, resorting to what is typically referred to as requests for "Mutual Legal Assistance" for requesting and obtaining evidence for criminal investigations and prosecutions from a foreign sovereign state. Though India has Mutual Legal Assistance Treaties

(MLATs) agreements with 39 countries²⁸, India should focus on strengthening its MLATs and similar mechanisms for international law enforcement assistance.

2.139 One stakeholder opined that MLATs apart, assistance may be denied by either country (according to agreement details) for political or security reasons, or if the criminal offence in question is not equally punishable in both countries. To obviate such situations, especially if the data hosting country is not inclined to India's interests, local hosting of servers and storage should be mandated.

2.140 On the other hand, a few stakeholders were of the view that for national security and for the protection of sensitive personal data, the Authority should mandate the M2M cloud platform and application providers have their servers located in India and abide necessary licensing and IT Act terms for delivery of services, giving Indian customers the ability to delete the stored data, if needed. The confidential data of consumer must be protected and should not be transferred to another jurisdiction without the consent of the consumer. Many stakeholders in response to the M2M CP had submitted that from security perspective, the National M2M Roadmap prescribes all M2M gateways and application servers to be physically located in India. Also, by requiring them to host in India it will be possible to address the unforeseen security challenges.

Analysis

2.141 The available options and their advantages and disadvantages are listed below:

- (a) Restrict cross border data flow and mandate localization
Advantage

²⁸ <http://cbi.nic.in/interpol/mlats.php>

- Sensitive data (personal data, banking details, etc.) and data that could affect nation's security will remain in the country
- Efficient access to data for law enforcement purposes
- Easy for Law Enforcement Agencies (LEAs) to Lawful Intercept.
- Create Jobs
- Service provider would be required to follow Indian laws
- Infrastructure development

Disadvantage

- Very high cost for service provider -discourage investment
- trade barrier -impact the export market if other countries start imposing such restrictions
- inferior QoS as the interplay of many platforms cause issues in many aspects
- slow implementation -delay innovation
- Forced localization undermines competitiveness

(b) Allow cross border data flow

Advantage

- Encourage investments
- Economies of scale -beneficial for all type and size of companies
- Allow many small and medium-sized businesses to reach new customers inexpensively
- Allows companies to allocate resources more efficiently, access foreign markets, and participate in global supply chains
- Facilitate economic growth, reduce the cost and time of doing business, and enable efficient and affordable services for consumers
- Allow companies to provide innovative pricing solutions, manage risks, and where appropriate, work with regulators to prevent fraud and protect consumers.

Disadvantage

- Creates jurisdictional challenges

- Sensitive personal data and data that could affect nation's security will move across national borders
 - Difficult for LEAs to Lawful Intercept.
 - Service provider wouldn't be obligated to follow Indian laws
- (c) Restrict cross border data flow and mandate localization of only those services which have high potential impact on national security or sensitive industry (Defence, Internal security, healthcare, finance etc)

2.142 As per the international experience, most of the countries allow cross border data transfer. The majority of the world's largest Internet companies are headquartered in the United States.

2.143 The government may foster the growth of data based businesses in India by allowing cross border data flow but at the same time critical data related to national security and sensitive data such as data related to healthcare and finance, needs to be protected. There is a need to identify services that contain critical and sensitive data and these may be mandated to locate data servers in India. This must be assessed on a case by case basis, as in many circumstances obtaining individuals consent may well be sufficient provided that the data does not involve national secrets or violate national security. The government has to task some organization to identify critical and sensitive services which requires data localization.

2.144 The security threats are evolving and are in dynamic stage. The government should address them dynamically. In today's connected world, free movement of data is important to its appropriate place and to where it is needed. However protection of critical and sensitive data cannot be neglected. Instead of restricting cross border data flow, the government should regulate it. To address the difficulties faced by

LEAs to Lawful Intercept, the government should focus on increasing and strengthening MLATs.

2.145 According to Google transparency²⁹report³⁰, for the period of January to June 2016, the number of requests made by Indian Government for disclosure of user data from Google accounts or services was 3452. Out of which 55% of the requests were answered with some data. This shows that not all the requests were responded as required.

2.146 The MLATs can be considered as a solution for law enforcement agencies, for the purpose of gathering and exchanging information in an effort to enforce public or criminal laws but they are not always successful because assistance may be denied by either country (according to agreement details) for political or security reasons, or if the criminal offence in question is not equally punishable in both countries. In order to overcome this, government should allow data transfer to only those countries where there is adequate jurisdictions to provide data privacy and security and India also has MLATs with them.

2.147 Issues relating to cross border data flow can also be addressed to large extent by rapidly developing the data centre's and associated data analytics sector in the country. Availability of such facilities within the country would not only promote the use of local facilities for data processing but also help in signing of MLATs on fairer terms.

2.148 As brought out in para 1.9, Committee of Experts headed by Justice B N Srikrishna would be addressing the larger issues related to data protection framework applicable in general to all sectors of the economy. Since the issue of cross-border data flow is pertinent to all the sectors of the economy and would be addressed by the committee

²⁹ A transparency report is a statement issued on a regular basis by a company, disclosing a variety of statistics related to requests for user data, records, or content. Transparency reports generally disclose how frequently and under what authority governments have requested or demanded data or records over a certain period of time.

³⁰ <https://www.google.com/transparencyreport/userdatarequests/IN/>

of experts, the Authority, at this juncture, has decided not to make any recommendations on the issue of cross-border data flow.

Chapter 3: Summary of recommendations

3.1 Personal Data

The Authority recommends that: (Refer paragraph 2.20)

(a) The definitions of “Data” as provided under Information Technology Act, 2000, and “Personal Information” and “Sensitive Personal Data and information” as provided under Sensitive Personal Data and Information Rules, 2011, as reproduced below, are adequate for the present.

- (i) "Data"** – defined in section 2(1)(o) of the *Information Technology Act, 2000* as a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.
- (ii) "Personal information"**– defined in the *Sensitive Personal Data and Information Rules, 2011* as any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.
- (iii) "Sensitive personal data or Information"**– defined in the *Sensitive Personal Data and Information Rules, 2011* as such personal information which consists of information relating to:- password, financial information such as bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; biometric information; any detail relating to the

above clauses as provided to body corporate for providing service; and any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise: provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

- (b) Each user owns his/ her personal information/ data collected by/ stored with the entities in the digital ecosystem. The entities, controlling and processing such data, are mere custodians and do not have primary rights over this data.**
- (c) A study should be undertaken to formulate the standards for anonymisation/ de-identification of personal data generated and collected in the digital eco-system.**
- (d) All entities in the digital eco-system, which control or process the data, should be restrained from using metadata to identify the individual users.**

3.2 Sufficiency of existing Data Protection Framework

The Authority recommends that: *(Refer paragraph 2.39)*

- (a) The existing framework for protection of the personal information/ data of telecom consumers is not sufficient. To protect telecom consumers against the misuse of their personal data by the broad range of data controllers and processors in the digital ecosystem, all entities in the digital ecosystem, which control or process their personal data should be brought under a data protection framework.**

- (b) Till such time a general data protection law is notified by the Government, the existing Rules/ License conditions applicable to TSPs for protection of users' privacy be made applicable to all the entities in the digital ecosystem. For this purpose, the Government should notify the policy framework for regulation of Devices, Operating Systems, Browsers and Applications.
- (c) Privacy by design principle should be made applicable to all the entities in the digital ecosystem viz, Service providers, Devices, Browsers, Operating Systems, Applications etc. The concept of "Data Minimisation" should be inherent to the Privacy by Design principle implementation. Here "Data Minimisation" denotes the concept of collection of bare minimum data which is essential for providing that particular service to the consumers.

3.3 User Empowerment

The Authority recommends that: *(Refer paragraph 2.59)*

- (a) The Right to Choice, Notice, Consent, Data Portability, and Right to be Forgotten should be conferred upon the telecommunication consumers.
- (b) In order to ensure sufficient choices to the users of digital services, granularities in the consent mechanism should be built-in by the service providers.
- (c) For the benefit of telecommunication users, a framework, on the basis of the Electronic Consent Framework developed by MeitY and the master direction for data fiduciary (account aggregator) issued by Reserve Bank of India, should be notified for telecommunication sector also. It should have provisions for revoking the consent, at a later date, by users.

- (d) **The Right to Data Portability and Right to be Forgotten are restricted rights, and the same should be subjected to applicable restrictions due to prevalent laws in this regard.**
- (e) **Multilingual, easy to understand, unbiased, short templates of agreements/ terms and conditions be made mandatory for all the entities in the digital eco-system for the benefit of consumers.**
- (f) **Data Controllers should be prohibited from using “pre-ticked boxes” to gain users consent. Clauses for data collection and purpose limitation should be incorporated in the agreements.**
- (g) **Devices should disclose the terms and conditions of use in advance, before sale of the device.**
- (h) **It should be made mandatory for the devices to incorporate provisions so that user can delete such pre-installed applications, which are not part of the basic functionality of the device, if he/she so decides. Also, the user should be able to download the certified applications at his/ her own will and the devices should in no manner restrict such actions by the users.**
- (i) **Consumer awareness programs be undertaken to spread awareness about data protection and privacy issues so that the users can take well informed decisions about their personal data.**
- (j) **The Government should put in place a mechanism for redressal of telecommunication consumers' grievances relating to data ownership, protection, and privacy.**

3.4 Data Privacy and Security of Telecom Networks

The Authority recommends that: *(Refer paragraph 2.103)*

- (a) Department of Telecommunication should re-examine the encryption standards, stipulated in the license conditions for the TSPs, to align them with the requirements of other sectors.**
- (b) To ensure the privacy of users, National Policy for encryption of personal data, generated and collected in the digital eco-system, should be notified by the Government at the earliest.**
- (c) For ensuring the security of the personal data and privacy of telecommunication consumers, personal data of telecommunication consumers should be encrypted during the motion as well as during the storage in the digital ecosystem. Decryption should be permitted on a need basis by authorized entities in accordance to consent of the consumer or as per requirement of the law.**
- (d) All entities in the digital ecosystem including Telecom Service Providers should be encouraged to share the information relating to vulnerabilities, threats etc in the digital ecosystem/ networks to mitigate the losses and prevent recurrence of such events.**
- (e) All entities in the digital ecosystem including Telecom Service Providers should transparently disclose the information about the privacy breaches on their websites along with the actions taken for mitigation, and preventing such breaches in future.**
- (f) A common platform should be created for sharing of information relating to data security breach incidences by**

all entities in the digital ecosystem including Telecom service providers. It should be made mandatory for all entities in the digital ecosystem including all such service providers to be a part of this platform.

- (g) **Data security breaches may take place in-spite of adoption of best practices/ necessary measures taken by the data controllers and processors. Sharing of information concerning to data security breaches should be encouraged and incentivized to prevent/ mitigate such occurrences in future.**

List of Abbreviations

API	Application Programming Interface
App(s).	Application(s)
BPO	Business Promotion Offices
CERT-in	Indian Computer Emergency Response Team
CP	Consultation Paper
DoT	Department of Telecommunication
EU-GDPR	European Union- General Data Protection Regulation
GDP	Gross Domestic Product
IP	Internet Protocol
IRDA	Insurance Regulatory and Development Authority
ISO	International Organization for Standardization
IT	Information Technology
LEA	Law Enforcement Agency
M2M	Machine-To-Machine
MAC	Medium Access Control
MLAT	Mutual Legal Assistance Treaties
MNC	Multi National Company
NCPR	National Consumer Preference Register
NDSAP	National Data Sharing and Accessibility Policy
OHD	Open House Discussion
OTT	Over the Top
PFRDA	Pension Fund Regulatory and Development Authority
PID	Personal Identity Data

QoS	Quality of Service
R&D	Research and Development
RBI	Reserve Bank of India
SEBI	Securities and Exchange Board of India
SPDI	Sensitive Personal Data and Information
TSP	Telecom Service Provider
UASL	Universal Access Service License
UL	Universal License

On the TRAI's recommendations on Privacy

The talk of the tech policy circles in Delhi these days is about the delays in the release of the Srikrishna Committee report on Privacy: Will they release a law, or will it just be recommendations? Have the recommendations been delayed because the committee is indecisive now about data localisation, given the reaction to the RBI's seemingly "out of the blue" diktat regarding localisation of financial transaction data? Is the iSpirt/UIDAI/"Nandan-Nilekani-friendly" faction in the Srikrishna Committee digging its heels in about data localisation? Or is it that they don't want it to affect Aadhaar and Justice Srikrishna does? Is there a point to the Srikrishna Committee, since the bill may never get tabled: the opposition may not let the Monsoon session to run in Parliament, and there's very little chance of any work in the winter session?

In that context, the TRAI's recommendations are very important, especially given that the TRAI Chairman is the former CEO of the UIDAI, the fact that the TRAI took on this consultation suo moto, and there's talk of him possibly becoming head of India's first data protection authority after his term finishes at the TRAI. These recommendations are being seen as a signal for what's to come from the Srikrishna Committee.

Issues that the TRAI has avoided

Before we get into what the TRAI has recommended, I think it's worth looking at what the TRAI has avoided talking about:

- Data Localisation,
- Cross-border data flows,
- Legitimate Exceptions to privacy,
- Lawful interception,
- responsibilities of data controllers and technology-based audits.

These are all contentious topics and there, from what we've heard, is a lot of pressure from law enforcement agencies, for access to user data. This TRAI, which has been especially focused on consumer interest, has avoided stepping into some potential minefields.

Most importantly, it hasn't gone into issues of mass surveillance and its prevention, offered no conclusive comments on exceptions to the privacy law, saying that because the privacy framework is under development, "the Authority has decided not to make any recommendations."

Uhh... pretty much everything that the TRAI has covered in this paper is a part of the privacy framework under development, and this isn't a sufficient reason for the TRAI to opt out from commenting, while commenting on everything else. Somewhere in the paper, it does say that "Since the data is collected by private as well as government entities, the data protection framework should be equally applicable to both the Government as well as private entities", which is

a welcome development, given that there would have been push-back regarding this from the Home ministry.

That said, the TRAI has done a fairly decent analysis of issues pertaining to cross-border data flows and data localisation, without taking a stand on it.

TRAI Recommendations on privacy and data protection

1. Ownership of personal data:

Each user owns his/ her personal information/ data collected by/ stored with the entities in the digital ecosystem. The entities, controlling and processing such data, are mere custodians and do not have primary rights over this data.

The TRAI says that data isn't just a property and "...it would appear illogical/ inequitable to permit complete transfer of rights over an individual's personal data. This would imply that, the personal data can no longer be used/ accessed by the data owners – a situation which is quite clearly untenable. In the circumstances, there must be a recognition that while data controllers may indeed collect and process personal data, this must be subject to various conditions and obligations – including importantly, securing explicit consent of the individual, using the personal data only for identified purposes, etc. The entity that has control over personal data would be responsible for compliance with data protection norms."

The TRAI has recommended a study to formulate standards for anonymisation and de-identification of personal data. In addition, it has said that

All entities in the digital eco-system, which control or process the data, should be restrained from using metadata to identify the individual users.

How exactly does the TRAI expect all entities in the digital ecosystem to be restrained from using metadata from identifying individual users?

2. Jurisdiction of TRAI's recommendations:

Two aspects of the TRAI's recommendations appear to go beyond its remit. It says:

- Till such time a general data protection law is notified by the Government, **the existing Rules/ License conditions applicable to TSPs for protection of users' privacy be made applicable to all the entities in the digital ecosystem.** For this purpose, the Government should notify the policy framework for regulation of Devices, Operating Systems, Browsers, and Applications.

These recommendations, coupled with the recommendations regarding devices – of allowing users to delete pre-installed apps, and previous comments from the TRAI Chairman regarding devices being a part of the telecom ecosystem, appear to be seeking to extend the TRAI's jurisdiction beyond telecom. Remember that when this paper came out, it appeared to be more about the Internet than telecom, and we had pointed out that the TRAI does not have jurisdiction over the Internet. No doubt that these recommendations are well-meaning, but privacy isn't really a part of the TRAI's or the DoT's remit. That should be with MEITY, in the absence of a Data Protection Authority.

A positive development is the TRAI's suggestion from the TRAI:

Since the data is collected by private as well as government entities, the data protection framework should be **equally applicable to both the Government as well as private entities.**

3. Data minimisation & Privacy by Design:

Privacy by design principle should be made applicable to all the entities in the digital ecosystem viz, Service providers, Devices, Browsers, Operating Systems, Applications etc. The concept of “Data Minimisation” should be inherent to the Privacy by Design principle implementation. Here “Data Minimisation” denotes the concept of collection of bare minimum data which is essential for providing that particular service to the consumers.

4. Data portability and deletion

The Right to Data Portability and Right to be Forgotten are restricted rights, and the same should be subjected to applicable restrictions due to prevalent laws in this regard.

The TRAI here appears to conflate the Right to be Forgotten, which refers to removal from search engine index with data deletion. That said, empowering users to delete telecom data, and port their data (and not just from their numbers), is a welcome move.

5. Notice and Consent

This is a big one. As we've discussed, consent is broken, and the TRAI has recommended that for telecom users,

5.a Consent mechanism on the basis of the Electronic Consent Framework from MEITY

“In order to ensure sufficient choices to the users of digital services, granularities in the consent mechanism should be built-in by the service providers.” Apart from that, the TRAI has recommended that a framework, “on the basis of the Electronic Consent Framework developed by MeitY and the master direction for data fiduciary (account aggregator) issued by Reserve Bank of India, should be

notified for telecommunication sector also. It should have provisions for revoking the consent, at a later date, by users.”

5b: Multilingual agreements: The TRAI has recommended that agreement/terms and conditions be “Multilingual, easy to understand, unbiased, short templates” for “all the entities in the digital eco-system”

5c. No pre-ticked boxes:

Data Controllers should be prohibited from using “preticked boxes” to gain users consent. Clauses for data collection and purpose limitation should be incorporated in the agreements.

5d. Devices and consent:

(g) Devices should disclose the terms and conditions of use in advance, before sale of the device.

(h) It should be made mandatory for the devices to incorporate provisions so that user can delete such pre-installed applications, which are not part of the basic functionality of the device, if he/she so decides.

Also, the user should be able to download the certified applications at his/ her own will and the devices should in no manner restrict such actions by the users.

6. Improvement in Encryption standards

This is one of the issues that we had raised at the open house on privacy: That data sent over telecom networks is not secure, and we need strong privacy recommendations to enable security of that data. The TRAI recommends that:

- To ensure the privacy of users, National Policy for encryption of personal data, generated and collected in the digital eco-system, should be notified by the Government at the earliest.
- For ensuring the security of the personal data and privacy of telecommunication consumers, **personal data of telecommunication consumers should be encrypted during the motion as well as during the storage in the digital ecosystem.**
- Decryption should be permitted on a need basis by authorized entities in accordance to consent of the consumer or as per requirement of the law.

This is a very welcome suggestion from the TRAI, and it's about time that this issue got addressed. That said given the mess that the last (now withdrawn) Draft Encryption Policy was, this needs to be looked at carefully.

7. Breach and notification

All entities in the digital ecosystem including Telecom Service Providers should be encouraged to share the information relating to vulnerabilities, threats etc in the digital ecosystem/ networks to mitigate the losses and prevent recurrence of such events.

All entities in the digital ecosystem including Telecom Service Providers should transparently disclose the information about the privacy breaches on their websites along with the actions taken for mitigation, and preventing such breaches in future.

A common platform should be created for sharing of information relating to data security breach incidences by all entities in the digital ecosystem including Telecom service providers. It should be made mandatory for all entities in the digital ecosystem including all such service providers to be a part of this platform.

Data security breaches may take place in-spite of adoption of best practices/ necessary measures taken by the data controllers and processors. Sharing of information concerning to data security breaches should be encouraged and incentivized to prevent/ mitigate such occurrences in future.

This is a measured approach: one issue with breach notifications is that companies that get breached are afraid of harassment from law enforcement agencies. It's a tricky thing to deal with: at one level, it is important to ensure that companies try and protect user data, and hence penalties are a means of ensuring that they behave responsibly. At another level, the fear of penalties (and loss of business) prevent companies from disclosing breaches to law enforcement and customers.

All in all, these are welcome recommendations from the TRAI. Download your copy [here](#).

Key aspects of the Personal Data Protection Bill, 2019

India's Personal Data Protection Bill has been introduced in the Parliament's lower house, the Lok Sabha, and is likely to be sent to a Joint Parliamentary Committee, comprising of 30 members (20 from the Lok Sabha, 10 from the Rajya Sabha). After the committee makes its recommendations, it will be tabled in the Lok Sabha for passing, after which it will be sent to the Rajya Sabha (the upper house of Parliament) for passing, and then to the President for his assent before it becomes a law.

This law has been two years in the making, and will lead to the creation of a Data Protection Authority in India, the imposition of norms on collecting and processing of data, as well as the cross-border transfer of data. Key aspects of the bill:

1. Kinds of personal data:

The Bill regulates 3 categories of data – Personal Data, Sensitive Personal Data, and Critical Personal Data.

- Sensitive personal data may be transferred for processing outside India with the user's explicit consent and the Data Protection Authority's or Central government's permission , but needs to be stored only in India. Sensitive personal data includes financial data, health data, sexual orientation, transgender status, case/tribe, and religious or political beliefs. The Central government and DPA can together also notify further kinds of data as sensitive personal data. "Passwords" have been removed from the list of sensitive personal data listed in the bill.
- Critical personal data has not been defined and what it is will be notified by the Central government; it can be processed only in India.

The Bill dilutes data localisation requirements, as envisaged in the Srikrishna draft bill, and mandatory mirroring of personal data has also been removed.

2. Right to be Forgotten

The Bill gives a user the right to be forgotten, that is to stop their data from being disclosed if the purpose of data collection has been served, if the user withdrew consent, or the data was disclosed illegally. The user can make a complaint to Data Protection Authority, who will then order the data fiduciary to remove the user's data.

3. Significant Data Fiduciaries

The Data Protection Authority can notify any data fiduciary as a significant data fiduciary on the basis of the volume and sensitivity of personal data being processed, the data fiduciary's turnover, risk of harm by processing by the data fiduciary, use of new technologies for processing, any other factor causing harm from such processing.

A significant data fiduciary will have to carry out a Data Protection Impact Assessment, in order to undertake any processing involving new technologies, use of sensitive personal data such as biometric data, etc. Such a fiduciary also has to undergo compliance evaluation by a data auditor, who is appointed by the Data Protection Authority.

4. Social media intermediaries and verification

If any “social media intermediary” has a certain number of users, and can impact electoral democracy, India’s security, sovereignty or public order, can be notified by the Central government and DPA as a “significant data fiduciary”. Different thresholds will be notified for different classes of social media intermediaries. A social media intermediary has been defined as “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”. This does not include intermediaries which enable commercial or business transactions, provide access to the internet, email services, search engines, and online encyclopedias.

Social media intermediaries, classified as significant data fiduciaries, will now have to give **account verification options to willing users**, and **such users will be given a visible mark of verification**. This will be voluntary.

5. Non-personal Data

The bill empowers the Central government to direct any data fiduciary or processor to provide anonymised personal data or other non-personal data “to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government”.

6. Consent manager

The bill introduces the concept of consent manager; users can use it to give or withdraw consent to the data fiduciary. Consent manager is defined as a data fiduciary “which enables a data principal to gain, withdraw, review, and manage his consent through an accessible, transparent, and interoperable platform”.

7. Personal Data

Personal data’s definition has been expanded to include online and offline data about a natural person, “or any combination of such features with any other information”, and to include any “inference drawn from such data for the purpose of profiling”.

8. Exemptions to the government

The Indian government can exempt any government agency from the Act for reasons of national security, integrity & sovereignty, public order, friendly relations with foreign states, and for preventing any cognizable offence relating to the above.

Apart from exemptions to government agencies, certain rights of users will be suspended if personal data is processed for law enforcement, judicial reasons, journalism, and for personal reasons.

9. Data Protection Authority

The independence of the regulator has been significantly reduced, in comparison with the last bill. The selection committee — which will make recommendations to the government on appointment of DPA's members — are now made up of government officials, including the Cabinet Secretary, Law Secretary, and MeitY secretary. In the earlier version of the bill, this committee consisted of members of the judiciary, including the Chief Justice of India as chairperson. Users have the right to appeal to the Appellate Tribunal, if they are dissatisfied with orders made by an officer of the Data Protection Authority.

10. Processing without consent:

Personal data may be processed without consent for performance of a state function, including for provision of state services and in response to medical emergency, for employment-related purposes. Personal data can also be processed without consent for other “reasonable purposes”, including for prevention of illegal activities, whistle-blowing, credit scoring, debt recovery, and importantly – operation of search engines.

11. Children’s data privacy:

Data fiduciaries can process a child’s personal data only after verifying their age, and obtaining the consent of their parent or guardian. The Data Protection Authority can classify any data fiduciaries who operate services directed at children, or process large amount of children’s personal data as a “guardian data fiduciary”.

A guardian data fiduciary will be barred from profiling, tracking or monitoring the behaviour of children, target ads at children, or carry out any other processing that can cause significant harm to the child.

Follow our live-blog and Twitter handle for updates.

Decoding the Personal Data Protection Bill, 2019: A new data governance framework for India | Ikigai Law

The Personal Data Protection Bill, 2019 (“Bill”) was introduced in the Lok Sabha (lower house of the Indian Parliament) on 10 December 2019. Once enacted, this Bill will require a large number of companies (both Indian and foreign) to revamp their operational practices. This post provides an overview of the major practical concerns raised by this Bill.

1. Who is affected by this Bill?

In addition to Indian companies, the Bill applies to: (i) companies that process data in India, (ii) companies outside India that process data in connection with a business in India, and (iii) companies outside India that process data in connection with any activity which involves profiling of people within the territory of India. Therefore, even businesses outside India can be covered by this Bill.

2. Will the Bill change how companies should treat personal data?

The Bill lays down standards for how companies should process personal data, and imposes obligations on them for this purpose. Processing in this context means the use, collection, recording, organisation, storage, alteration, indexing, disclosure and erasure of personal data, amongst other things. Since many tech companies perform these operations on personal data, they will be required to comply with the new obligations under this Bill. Operationalising the privacy framework under the Bill will require companies to make significant changes to their data collection and processing practices. For example, companies will now need to take fresh consent from their users for processing their data, as per the detailed consent requirements under the Bill. Companies will also need to prepare a ‘privacy by design’ policy. This policy should describe: business practices and technical systems adopted to protect personal data, strategies to anticipate and avoid ‘harm’ to individuals, and how individuals’ interests are accounted for at every stage of data-processing.

3. What about non-personal data?

The Bill allows the government to direct companies to share anonymised personal data/non-personal data for improving service delivery or formulating policies. Non-personal data is defined as any data other than personal data.

4. Does the Bill restrict cross-border transfers of data?

Companies will not be able to freely store and transfer all types of personal data outside India once the Bill is enacted. Some types of personal data, which will be classified as critical personal data by the government, must be stored in

India, and can only be transferred in limited cases (eg., for emergency/ health purposes). Sensitive personal data must also be stored in India, though it can be transferred outside India subject to certain conditions being met.

5. Will companies need to change the manner in which they obtain user consent for processing personal data?

The current data protection framework in India requires companies to obtain user consent for data processing only where sensitive personal data (eg., financial data) is involved. Collection and processing of personal data does not need consent, and consent need not be obtained through a notice. This will change if the Bill is enacted in its current form. This is because the Bill requires companies to acquire user consent in order to process even their personal data (for eg., names, addresses, age etc.). In order to be considered valid, consent must be freely given, informed, specific, capable of being withdrawn and indicated through affirmative action (meaning that ‘pre-checked’ consent boxes may no longer work). While seeking user consent, companies will have to provide users with detailed notices at the time of collection of data. Additionally, companies cannot make the provision of any good/services or their quality conditional on consent. Thus, access to websites or user registration cannot be made conditional on consent, unless the data to be collected is necessary for the provision of such services.

6. Should companies be concerned by the classification of sensitive personal data under the Bill?

All financial data, health data, biometric data, genetic data, data indicating religious/political beliefs/sexual orientation or caste/tribe status are considered sensitive personal data under the Bill. The Bill imposes stricter standards for processing such data as compared to the standards under India’s current data protection framework. For example, companies collecting or processing such data will need explicit user consent – meaning that they will have to inform users of the consequences of processing their data and inform them of processing which is likely to cause them significant harm, in addition to the regular notice and consent requirements. This can have impractical effects for the everyday use of publicly information like surnames that reveal caste/tribe or statements reflecting political/religious opinions available online – it appears that companies will need users’ explicit consent for collection and use of even this freely available data.

7. Will the Bill affect how companies should treat children’s personal data?

The current data protection framework does not impose additional requirements on companies that process children’s data. Once the Bill is passed, companies will have to seek parental/guardian consent and verify children’s age before processing their data.

8. Are there any restrictions on the amount of data that can be

collected by companies?

The Bill allows companies to collect personal data only for purposes that are clear, specific, lawful and communicated in advance. Additionally, companies must only collect data that is necessary for processing. This could create difficulties – it may not always be possible to determine the exact purpose of data collection beforehand. For instance, with devices that work in an Internet of Things (“IoT”) ecosystem, the purposes for which data may be used are constantly evolving, and so it could be difficult to spell out exactly what purpose the data is going to be collected for.

9. Does the Bill apply different standards to different companies?

The Bill allows the government to notify certain companies as ‘significant data fiduciaries’ based on factors like the volume of personal data they process, the sensitivity of such data, their turnover etc. Once classified as significant data fiduciaries, companies will have to comply with heightened obligations like conducting data protection impact assessments, appointing data protection officers, and in the case of social media companies, enabling their users to voluntarily verify their accounts. This means that large companies that process large volumes of personal data and enjoy high turnovers can be notified as significant data fiduciaries which will have to comply with these heightened obligations.

10. Does the Bill allow for innovation in emerging technologies that involve the use of data?

The Bill allows the Data Protection Authority to create a data sandbox for the purpose of encouraging innovation in artificial intelligence, machine learning or any other emerging technology in public interest. Companies participating in the sandbox will be able to avail of certain exemptions.

11. Who will regulate this new law?

The Data Protection Authority will be responsible for the enforcement of the Bill once it is enacted. It has wide-ranging powers – including the power to require certain entities to conduct mandatory data protection impact assessments and the power to permit cross-border transfers in certain cases.

12. What are the consequences of non-compliance with the Bill?

Non-compliance with the Bill can attract penalties of up to INR 15 crores or 4% of worldwide turnover, whichever is higher.

[This post has been authored by Tuhina Joshi, Associate, Ikigai Law, with inputs Sreenidhi Srinivasan, Senior Associate, Ikigai Law.]

Key Changes in the Personal Data Protection Bill, 2019 from the Srikrishna Committee Draft

The Personal Data Protection Bill, 2019 (“the PDP Bill, 2019”) was tabled in Parliament on December 11th, 2019. The PDP Bill, 2019 has brought in some new clauses – compliance obligations for social media companies and enhanced State power to exempt any government agency from the purview of the Bill; relaxed some existing provisions – done away with mandatory mirroring requirements for all personal data and done away with certain offences for transferring/ selling personal data; and in some cases removed extant requirements such as the creation of the Data Protection Funds, as compared to the Draft Personal Data Protection Bill, 2018, which was released last year.

Some of the key changes brought in by the PDP Bill, 2019 are as follows:

- 1. Social Media Intermediaries and voluntary verification of accounts (Sec. 26 and 28 of the Bill)**

The PDP Bill, 2019 extends the obligations of significant data fiduciaries to another class of entities called the social media intermediaries (“SMIs”). The Bill defines SMIs to mean intermediaries who primarily/ solely enable online interaction between two or more users and allow them to create, upload, share, disseminate, modify or access information using its services (it specially excludes entities like – e-commerce platforms, TSPs/ ISPs, search engines, cloud service providers, online encyclopedias, and email services from the definition of SMIs). Another qualification for an entity to be an SMI is – the likelihood or actual impact on electoral democracy, security of the State, public order or the sovereignty and integrity of India [see Sec. 26(4)].

In addition to obligations such as – data protection impact assessments (Sec. 27), maintenance of records (Sec. 28), audit of policies (Sec. 29), and appointment of a data protection officer (Sec. 30), which are applicable to all significant data fiduciaries, SMIs are required to provide an option to users (registering from India or using the services in India) for voluntary verification of their accounts [the methods of such voluntary verification will be notified by the Central Government as per Sec. 93(1)(d) of the Bill]. Verified user accounts will be marked with a demonstrable verification mark [See Sec. 28(4)]. As per Sec. 29, data auditors are required to evaluate SMIs for timely implementation of their obligations under account verification norms.

Social media verification requirements are misplaced in data protection legislation. As under existing provisions [see Sec. 26(1)] social media companies could easily fall under the ambit of significant data fiduciaries, the only basis for this distinct classification could be to introduce account verification mechanisms. This new concept of verification of social media accounts does not belong in a comprehensive data protection regulation and must be removed.

2. Central Government can Exempt any Government Agency from the Bill (Sec. 35 of the Bill)

Sec. 42 of the Draft Personal Data Protection Bill, 2018 (“the Srikrishna Bill”) allowed access of personal data to the Government for security purposes based on principles of necessity and proportionality and on the basis of authorisation under law. The provision for Government access to personal data under the PDP Bill, 2019 (Sec. 35) is wider, gives the Central Government power to exempt any government agency from the purview of the Bill (all or select provisions) and does not codify the principles of necessity and proportionality as determinants to access.

Sec. 35 of the PDP Bill, 2019 effectively enhances existing surveillance powers of the government and gives the State over arching authority to access personal data. This provision enables government surveillance projects like the NAT-GRID, CMS, and the nationwide facial recognition program, effectively enabling the Government to collect and process any category of personal data per their requirements. Even the Srikrishna Committee Report recognised that unfettered access to the Government of personal data, without adherence to established safeguards (such as necessity and proportionality as expounded in the privacy judgment of the Supreme Court – *Puttaswamy*) is potentially unconstitutional. Granting access of personal data to the Government, without appropriate safeguards and judicial oversight is against established constitutional principles and should not form part of the PDP Bill, 2019.

3. Dilution of Data Localisation Requirements (Sec. 33 and 34 of the Bill)

The mandatory requirement for storing a mirror copy of all personal data in India as per Sec. 40 of the Srikrishna Bill has been done away with in the PDP Bill, 2019. Localisation requirements are only on sensitive and critical personal data (stored in India with conditions for transfer overseas). Critical personal data may only be processed in India [See Sec. 33(2)]. Sensitive personal data (“SPD”) may be transferred outside India based on explicit consent and a) if the transfer is made per a contract or intra-group scheme (approved by the data protection authority); or b) Central Government allows transfer to a country, entity or international organization; (requisite safeguards for protection of such personal data are prescribed under these provisions) or c) data protection authority may allow a transfer of SPD for specific purposes.

Similarly, for critical personal data, transfers may be allowed for health or other emergency services or where the Central Government approves transfers to a country, entity or international organization.

Though, removing the mandatory mirroring requirement is an appropriate change, users/ data principals should be given rights over where they wish to store their personal data and the State should not impose restrictions on transfer of such data, specially once explicit consent has been given.

4. The Right to Erasure (Sec. 18 of the Bill)

The Srikrishna Bill did not contain a right to erasure, even under the right to be forgotten (“RTBF”) (See Sec. 27 of the Srikrishna Bill). The PDP Bill, 2019 has brought the right to erasure alongside the right to correction of personal data [See Sec. 18(1)(d)]. The data principal may request data fiduciaries for a right to erasure of personal data when such data is no longer necessary for the purpose of processing. Data fiduciaries may refuse such requests for erasure, but data principals may require fiduciaries to take reasonable steps to indicate, alongside the relevant personal data, that the same is disputed by them.

This is a good inclusion as it enhances data principal rights to request the erasure of data which is no longer needed for the purpose of processing. Such a right was missing from Srikrishna Bill. A right to erasure should also be incorporated under the RTBF (under Sec. 20 of the PDP Bill, 2019), as presently, RTBF only includes a right to non-disclosure and not erasure.

5. Removal of Judicial Member from Selection Committee Recommending Members to the Data Protection Authority (Sec. 42 of the Bill)

The PDP Bill, 2019 has removed the inclusion of a judicial member (the Chief Justice of India or another Supreme Court Judge) from the selection committee which is empowered to give recommendations to the Central Government for the appointment of members of the Data Protection Authority (“the DPA”) [the Srikrishna Bill included a judicial member in the selection committee - see Sec. 50(2) of the Srikrishna Bill]. Now, as per Sec. 42(2) of the PDP Bill, 2019, the selection committee will comprise of – a) the Cabinet Secretary (who’s also the Chairperson); b) Secretary, Department of Legal Affairs; and c) Secretary, Ministry of Electronics and Information Technology.

The DPA is completely dependent on the Central Government for its formation and membership. Considering that the PDP Bill, 2019 applies to the Government agencies as well, the regulatory body, which is tasked with enforcement of the Bill, is not independent from the State.

To ensure the independence of the DPA, there should be sufficient involvement of judicial members in the selection committee as well as in the DPA. This will guarantee judicial review and will quell concerns of conflict of interest.

6. Central Government can direct Data Fiduciaries to share Anonymized Personal Data/ Non- Personal Data (Sec. 91 of the Bill)

Sec. 105 of the Srikrishna Bill, gave powers to the Central Government to formulate appropriate policies for the digital economy, including measures for its growth, security, integrity, prevention of misuse, in context to ‘non-personal data’. That Bill did not define what was meant by non-personal data or how was it to be utilized by the government. The PDP Bill, 2019, under Sec. 91, goes a step further – a) it defines non-personal data as data that does not fall

under the definition of personal data [for the definition of personal data see Sec. 3(28)]; and b) empowers the Central Government to direct any data fiduciary/processor to provide any anonymised personal data or 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.*” [See Sec. 91(2)]. Sec. 2(B) of the PDP Bill, 2019 specifies that the Bill would not apply to anonymised data, other than as provided by Sec. 91 – which enables the Central Government to request entities to convert personal data into anonymized data for their own use.

In September this year, the Ministry of Electronics and Information Technology, constituted an expert committee to deliberate over a data governance framework for the regulation of ‘non-personal data’. Till the report of this expert committee is published, it would not be appropriate for the PDP Bill, 2019 to include government access to non-personal/ anonymised data. The expert committee must invite recommendations from the public and give civil society an opportunity to comment on privacy rights related issues with anonymised/ non-personal data.

On the point of requesting anonymised and non-personal data by the Central Government from any data fiduciary, this may be an onerous demand on data fiduciaries. Applying anonymisation standards, specially for start-ups and SMEs may be a cumbersome task. There aren’t any safeguards appended to this provision. What if a data fiduciary does not properly anonymise personal data? Or shares non-personal data which can easily be turned into personally identifiable data by combining various data points? The Bill does not provide safeguards for such situations in the interest of privacy rights of data principals.

7. Transparency in Data Sharing and the Concept of Consent Managers (Sec. 17, 21, and 23 of the Bill)

Sec. 17(3) of the PDP Bill, 2019, gives rights to data principals to access, in one place, the identities of data fiduciaries with whom their personal data has been shared by any (other) data fiduciary. This potentially enables data principals to review the entities with whom their personal data has been shared by one particular data fiduciary. This right has been added under the clause for the right to confirmation and access (this right was contained in Sec. 24 of the Srikrishna Bill).

This bolsters the rights framework in the PDP Bill, 2019. Data principals shall have the right to know about all the entities which are processing/ sharing their personal data. This, clubbed with the right to withdraw consent enhances the rights of the data principals in terms of their informational privacy.

The PDP Bill, 2019, also introduces the concept of ‘consent managers’ [See Sec. 21(1) and 23] which was not present in the Srikrishna Bill. The term Consent Managers is not defined in the definitions clause of the Bill, but is defined under an explanation to Sec. 23 as – a data fiduciary which enables a data principal to gain, withdraw, review and manage their consent through

an accessible, transparent and interoperable platform. All consent management platforms are to be registered with the DPA [See Sec. 23(5)].

From a reading of the definition of consent managers, it seems like the PDP Bill, 2019 has introduced the concept of ‘consent dashboards’ as recommended by the Srikrishna Committee in its report. On the face of it consent management tools/ consent dashboards may help in reducing consent fatigue, but they might bring up fresh privacy challenges. A trail of metadata generated by consent dashboards might help create a detailed profile of an individuals user engagement online. Specially, when such management tools are required to be registered with the DPA, metadata generated by these tools may assist in profiling of citizens.

8. Definitions of Personal and Sensitive Personal Data [Sec. 3(28) and (36) of the Bill]

The PDP Bill, 2019 has expanded the definition of personal data to include inferred data. Sec. 3(28) includes - “... and shall include any inference drawn from such data for the purpose of profiling”.

Including inferred data for the purpose of profiling in the definition of personal data is a positive move as this will give the right to data principals to request data fiduciaries for such data as well (See Sec. 17 of the Bill).

The PDP Bill, 2019 has taken off ‘passwords’ from under the purview of sensitive personal data. This may be for the reason for easy transfer of such data outside India when read in conjunction with the data localisation clauses – Sec. 33 and 34 of the Bill.

9. Privacy by Design Policy (Sec. 22 of the Bill)

The PDP Bill, 2019 introduces a concept of a privacy by design policy. Every data fiduciary is required to prepare a privacy by design policy and have it certified by the DPA. There is a requirement on each data fiduciary to publish this privacy by design policy once it has been certified by the DPA.

10. Removal of offences for obtaining, transferring, or selling of personal/ sensitive personal data (Sec. 90 and 91 of the Srikrishna Bill)

Offences for obtaining, transferring or selling of personal/ sensitive personal data have been removed from the PDP Bill, 2019 as compared to the Srikrishna Bill.

[There are other changes in the PDP Bill, 2019, like – removal of an obligation on data fiduciaries to demonstrate adherence to the Bill {Sec. 11(2) of the Srikrishna Bill}; SPD has been removed from the employer processing exception {Sec. 13(1) of the PDP Bill, 2019}; there is strict mandate now for data protection officers to be located in India {Sec. 30(3) of the PDP Bill, 2019}; and there is an exemption from certain clauses of the Bill for regulatory sandboxes (Sec. 40 of the PDP Bill, 2019). We will cover all these in our detailed analysis of the Bill.]

Justice Srikrishna data protection draft bill is now public, highlights and what happens next

The panel headed by retired Justice BN Srikrishna has submitted its bill on data protection to the IT Ministry on Friday. The draft bill, titled the Personal Data Protection Bill, 2018, now has to be tabled in Parliament. It will be the basis of a data protection framework that prescribes conditions for how organisations should receive, handle, and process individuals' personal data in India, along the lines of laws like the EU's General Data Protection Regulation (GDPR).

The draft legislation has 15 chapters and lays out a framework for data-protection obligations, grounds for processing of personal and sensitive personal data, data principal rights, provisions to govern the transfer of data outside India and the creation of a data protection authority.

LIVE BLOG

Key highlights from the bill

- Personal data has been defined as data which makes an individual directly or indirectly identifiable. The definition does not specifically mention any particular form of data or attribute. The bill **excludes anonymized data** from the application of this law.
- Apart from defining personal data the bill **labels certain information as sensitive personal data** as it existed under SPDI (sensitive personal data and information) Rules of the IT act, this has been expanded to include passwords; financial data; health data; official identifier; sex life; sexual orientation; **biometric data; genetic data; transgender status; intersex status; caste or tribe; religious or political belief or affiliation.**
- The law will extend to data fiduciaries or data processors who operate outside the country, if they carry out processing of personal data in connection either with any business carried on in India, systematic offering of good and services to data principles in India, or any activity which involves profiling of data principals (individual users) within of India.
- Legal grounds for processing under the bill include consent, functions of state, compliance with law or order of court/tribunal, for prompt action in case of emergencies, purposes related to employment and reasonable purposes of the data fiduciary.
- The bill provides certain rights to the data principal (i.e. the individual) this includes the **right to confirmation and access, right to correction, right to data portability and right to be forgotten.**
- Platforms operating under this law will have to adhere to certain transparency and accountability measures. These include Privacy by design, data protection impact assessment, record keeping, appointing a data protection officer and data audits.

- The bill places **restrictions on cross-border transfers of data**. The bill mandates storing a mirror of all personal data within the territory of India. The bill also empowers the central government to classify any sensitive personal data as critical personal data and mandate its storage and processing exclusively within India.
- The bill establishes an **independent authority called the Data Protection Authority of India that is empowered to oversee the enforcement of the bill**. The adjudication process will be looked after by the adjudication wing of the Authority.
- The bill lays down financial penalties for non-compliance ranging from **Rs 5 crores or 2% of total worldwide turnover to Rs 15 crores rupees or 4% of the total worldwide turnover**.

H/T: DSCI for their document on Highlights of the Personal Data Protection Bill.

What happens next?

The bill will likely be introduced in Parliament soon. IT Minister Ravi Shankar Prasad said that the bill will be subject to further parliamentary review before going to the Cabinet for approval. “Once the bill will be tabled in parliament it is likely to pass without any major amendments as the government has a strong majority,” Meghnad S, creator of Consti-tuition and Sansad Watch, told MediaNama.

Opaque and ineffective consultations

One of the issues afflicting the committee has been the opacity and purported ineffectiveness of its public consultation process. Firstly the public consultation should have followed the release of the draft bill as this would have allowed all stakeholders to examine and comment on the proposals made. Holding the public consultation before the release of the report means that said stakeholders will not be able to address any flaws present in the draft legislation.

Secondly, copies of submissions sent to the committee have not been made public. In a town hall in Mumbai, Justice Srikrishna responded to a concern by MediaNama on stakeholder submissions not being made public, saying, “You give your comments. Why do you worry about what anyone else has to say?”

The IT Ministry also refused to share copies of the submissions in response to an RTI application filed by Medianama. The IT Ministry has also refused to hand over minutes of the committee’s meetings. The ministry in its response said that the submissions were “confidential” and “not available for public dissemination” without the consent of the submitting entity. With regards to the ‘minutes of the meetings,’ the ministry said that it cannot be shared under Section 8(1)(i) of the RTI act.

Government invites public comments on Srikrishna data protection bill

The IT Ministry has invited comments on the Srikrishna committee's data protection bill. Comments can be posted here till the 5th of September 2018, that is 20 days from now. This further consultation takes special significance due to the contentious nature of the draft bill — there were voices of dissent from within the committee that found place on its official report. The data protection bill's provisions on maintaining a copy of personal data in India and its stiff criminal penalties for breaches have also drawn criticism.

Read: All roads of data sovereignty lead to a dystopia

It's unclear if the comments to the draft bill collected by MeitY will be made public. Public comments solicited by the Srikrishna Committee prior to the bill's drafting stage were not made public. In fact, MeitY declined multiple RTI requests to publish stakeholder comments. It's also unclear if MeitY will hold a counter-comment stage of consultation, where stakeholders will be able to comment on each other's responses. This two-stage process is typical of TRAI consultations, where comments are made public and commented on in a counter-comment stage as a matter of process.

How the bill measures up

While comments to the Srikrishna Committee were not published, some organisations made their filings public voluntarily. Here's a comparison of the Srikrishna Committee's bill with the expectations of i) Dvara Research, which prepared a skeletal draft bill of its own, and ii) SaveOurPrivacy.in, a volunteers' collective spearheaded by the Internet Freedom Foundation (*Note: MediaNama editor and publisher Nikhil Pahwa is IFF co-founder and chairman*).

Ownership, consent, portability and localisation

Localisation is probably the most glaring departure from both business' and civil society's expectations. The committee's bill requires all entities to store a copy of an individual's personal data in India, which will have huge associated costs. Data ownership is not asserted as the sole domain of the data subject, which somewhat weakens the foundations of a data protection bill. Consent requirements are still stringent, though, with multiple requirements needed to be satisfied for the consent to be regarded as explicit. Portability is required as it is in the SaveOurPrivacy.in privacy code.

How do the Srikrishna Committee's recommendations measure up?			
Issue	Model Bill (SaveOurPrivacy.in)	Dvara Research	Srikrishna Committee Recommendations
Data localisation	No requirements on companies to store personal data within the country	Personal data can be stored abroad if the foreign country in question has appropriate safeguards	All personal data of Indian citizens must have at least one copy stored in India
Data ownership	Personal data belongs solely to the data subject, i.e., the person who the data is about	No comment	No comment
Notice & consent	"Unambiguous" consent is a must for storage and processing of personal data	Consent should be obtained for collecting personal data, and clear notice of what information is being collected — and how it is processed — should be provided	Informed, free, and specific consent is required to collect personal data. Notice needs to be provided as to what data is being collected and how it is used
Data portability	Users should be able to ask for their data in a commonly used format, and for the data controller to directly transfer that data to a different data controller, on demand	Users should have the right to port their data from one data controller to another without hindrance	Users should be able to ask for their data in a commonly used format, and for the data controller to directly transfer that data to a different data controller

© MEDIANAMA

Right to be forgotten, transparency, and surveillance

The Srikrishna Committee's bill includes a right to be forgotten. The Adjudicating Officer, who is appointed under the data protection authority of India, will process applications based on sensitivity and necessity, among other factors. Anonymised data is not regulated by the bill, provided that the anonymisation is irreversible (the word anonymisation is itself defined as irreversible in all the bills). While the civil society bills allow users to access a copy of their information, the Srikrishna Bill only allows for a *summary* of that information to be accessed. On surveillance, the bill partially prohibits use of personal data for "security of the State" but doesn't go as far as SaveOurPrivacy hoped it would in mandating oversight.

How do the Srikrishna Committee's recommendations measure up?			
Issue	Model Bill (SaveOurPrivacy.in)	Dvara Research	Srikrishna Committee Recommendations
Right to be forgotten	No provision, except in cases of sexual assault, kidnapping, or abduction — people generally don't have a right under this Code to have public information about them destroyed or de-indexed from search engines on reputational grounds	No provision	The right to be forgotten exists, and not just for search engines. Requests are processed by the Data Protection Authority of India
Anonymisation and Pseudonymisation	Retaining anonymised personal data beyond the original purpose for which it was collected requires consent of users, and anonymisation needs to be demonstrably irreversible.	Anonymised personal data is not regulated, provided the process of anonymisation is irreversible.	The Bill does not apply to anonymised data. Anonymisation needs to be irreversible, as is the case in the Model bill and Dvara's legislative document
Data transparency	Data subjects have a vast range of rights — the right to access personal data stored about them; the right to know the purpose of collection and usage of that data; and the right to find out if automated decision-making is taking place with their information.	Data subjects have the right to access personal data stored with processors, right to be informed if and why automated decision making is taking place, right to dispute or erase any information, right to know the data retention period	Data subjects have a right to access a summary of data held about them, and what is being done with that data
Surveillance	Requires significantly expanded oversight into how state surveillance and lawful interception is conducted, with requirements for oversight and destruction of data after it is no longer required	No provision	Partial prohibition on usage of personal data for the security of the State without due procedure

© MEDIANAMA

Penalties, data protection authority, and breaches

The bill goes farther than civil society expectations here by not only having stiff civil penalties, but also *criminal* penalties that could involve jail time. The bill sets up a data protection authority, but only one — individual states don't get an authority of their own as the SaveOurPrivacy code hoped. Processing requirements are consistent with civil society attempts, but there exist carve-outs with fewer consent standards in the committee's bill. Importantly, breaches don't have to be disclosed to the public — only to the data protection authority.

How do the Srikrishna Committee's recommendations measure up?

Issue	Model Bill (SaveOurPrivacy.in)	Dvara Research	Srikrishna Committee Recommendations
Penalties for data controllers	Collecting, using and sharing personal data without consent and following the procedures laid out in the bill can lead to a penalty of Rs 1 crore and/or imprisonment upto three years	No fixed penalty is prescribed in the legislative document. The "adjudicating body" has the discretion of slapping a proportional fine on data controllers	Penalties range from ₹1 crore to ₹5 crore, or 2–4% of global annual turnover. Criminal penalties exist too
Data protection authority	State and central privacy commissions headed by commissioners are constituted, looking into privacy violation cases and fine-tuning the policies that flow from the model	A data protection authority is set up, and its constitution and appointments are left to the central government. Appeals are filed to the Cyber Appellate Tribunal	The Data Protection Authority of India will be set up. It should be headed by someone with not less than ten years of experience in IT and data protection
Data processing	As a principle, processing has to be fair and lawful. That means getting explicit consent, and only using personal data that is necessary for the task at hand	Processing can only be done with consent, and that processing must be in line with the notice that was provided when the data was first collected	Processing of data should be fair, reasonable, and lawful. Consent should always be obtained, subject to exceptions carved out for government use of personal data
Data breaches	Breaches have to be disclosed to the regulator and companies need to periodically publish reports on data breaches	Data subjects must be informed of breaches of sensitive personal data – including the data controller responsible for the breach, the extent of breach, and so on	Harmful breaches need to be disclosed to data protection authority. The authority decides whether the breach should be made public or not

© MEDIANAMA

Please note: MediaNama is also hosting discussions on the Srikrishna data protection bill in Delhi and Bangalore on August 23rd and 30th 2018 respectively. Click here to apply to attend.

Highlights of Personal Data Protection Bill, 2018

The committee of experts under the chairmanship of Justice B.N. Srikrishna, has brought its deliberations to a close and handed over the draft protection of personal data bill for India to Ministry of electronics and information technology for circulation. The following summarises the key provisions of the bill:

1. **Change in terminology:** The known terms of references, i.e., "Data Subject" and "Data Controller", have been reformulated as "Data Principal" and Data Fiduciary", to emphasize greater accountability and trust between the two. [Section 3(13), Section (14)]
2. **Horizontal Application:** The proposed bill applies to both government and private entities. [Section 2(1)(b)]
3. **Extra-territorial Application:** The applicability of the law will extend to data fiduciaries or data processors not present within the territory of India, if they carry out processing of personal data in connection with (a) any business carried on in India, (b) systematic offering of good and services to data principles in India, or (c) any activity which involves profiling of data principals within the territory of India. [Section 2 of the Bill]
4. **Personal Data:** Personal data has been defined on the parameters of identifiability. The definition does not specifically mention any particular form of data or attribute. [Section 3 (35)]. The bill expressly mentions the exclusion of anonymized data from the application of the law. [Section 2(3) of the Bill]
5. **Sensitive Personal Data:** Definition of sensitive personal data as it existed under SPDI Rules¹, has been expanded to include passwords; financial data; health data; official identifier; sex life; sexual orientation; biometric data; genetic data; transgender status; intersex status; caste or tribe; religious or political belief or affiliation. [Section 3(35) of the bill]
6. **Grounds for Processing Personal Data:** The legal ground for processing under the bill include: (a) consent, (b) functions of state, (c) compliance with law or order of court/tribunal, (d) for prompt action in case of emergencies, (e) purposes related to employment and (f) reasonable purposes of the data fiduciary. [Chapter III]
7. **Grounds for Processing Sensitive Personal Data:** The legal grounds for processing SPD under the bill include: (a) explicit consent, (b) functions of state, (c) compliance with law or order of court/tribunal, (d) for prompt action in case of emergencies for passwords, financial data, health data, official identifiers, genetic data, and biometric data. [Chapter IV]

¹ Rule 3. Sensitive personal data or information.— Sensitive personal data or information of a person means such personal information which consists of information relating to;— (i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details ; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information.

8. **Personal and Sensitive Personal Data of Children:** Processing of personal and sensitive personal of children by data fiduciaries should be done in a manner that protects and advances the rights and best interests of the child. Data fiduciaries are required to establish mechanisms for age verification and parental consent.

Fiduciaries that operate commercial websites or online services directed at children or process large volume of children personal data would be classified as guardian data fiduciaries and barred from performing certain processing operations. [Section 23 of the Bill]
9. **Data Principal Rights:** The bill provides the data principal with the (a) right to confirmation and access, (b) correction, (c) data portability and (d) right to be forgotten. [Section 24, Section 25, Section 26, Section 27 of the Bill]
10. **Transparency and Accountability Measures:** Chapter VII of the bill lays down practices that regulated entities under the bill must implement. These include: (a) Privacy by design, (b) data protection impact assessment, (c) record keeping, (d) appointing a data protection officer and (e) data audits. Practices inscribed in (b) to (e) are to be carried about by data fiduciaries which can been classified as “significant data fiduciaries” by the Data Protection Authority.
11. **Transfer of Personal Data Outside India:** Section 40 under the bill places restrictions on cross-border data flows. Section 40 (1) mandates storing one serving copy of all personal data within the territory of India. While section 40 (2) empowers the central government to classify any sensitive personal data as critical personal data and mandate its storage and processing exclusively within India.
12. **Conditions for Transfer of Personal Data Outside India:** The transfer is made subject to standard contractual clauses or intra-group schemes that have been approved by the Authority, prescribed that transfers to a particular country, or to a sector within a country or to a particular international organisation is permissible by the central government, transfers permissible due to a situation of necessity, consent with respect to personal data and explicit consent with respect to sensitive personal data. These provisions do not extent to critical personal data. [Section 41 of the bill]
13. **Data Protection Authority of India:** The bill establishes an independent authority empowered to oversee the enforcement of the bill. The adjudication process will be looked after by the adjudication wing of the Authority. [Chapter X. Section 60]
14. **Penalties, Remedies and Offences:** The bill lays down penalties under chapter XI of the bill, ranging from five crore rupees or two per cent of total worldwide turnover to fifteen crore rupees or 4% of the total worldwide turnover. The Data principle under section 75 has the remedy to claim compensation for harm suffered as a result of any violation of any provision in the bill from the data fiduciary or the data processors. The bill inscribes certain offences under chapter XIII of the bill, which are punishable with imprisonment.

15. **Transition Provisions:** Section 97 of the bill provides a structured timeline for enforcement from the date enacted of act. The enforcement duration is 18 months from the date of enactment, other than section 40, the duration of enforcement for this provision would be notified by the central government.

The Personal Data Protection Bill, 2018 can be accessed here : <http://meity.gov.in/content/personal-data-protection-bill-2018>.

Data Protection Framework and committee Report can be downloaded here:
http://meity.gov.in/writereadda/files/Data_Protection_Committee_Report.pdf

Personal Data Protection Bill, 2019: Considering consent and offences

As the Joint Parliamentary Committee considers the Personal Data Protection Bill, 2019, MediaNama will publish a series of articles from legal experts focussing on the key aspects of the Bill and how they will affect users and companies. This is the first article in the series. Read our extensive coverage of the Bill here.

By Rishab Bailey and Vrinda Bhandari

The popular teahouse chain Chaayos has been in the news recently for using facial recognition technology ('FRT') at a number of its stores in Delhi and Bangalore. Chaayos uses this technology to create profiles of its customers. These profiles are then used to "remember" them on subsequent visits, enabling repeat orders and efficient payment.

It has been reported that Chaayos does not display any information about the use of the personal data (that is, the image) collected by the system, that there was no opt-out option presented to customers, and that there was no obvious way of deleting one's data from the system.

With the tabling of the Personal Data Protection Bill, 2019 ('Bill'), in Parliament, the use of FRT may soon be regulated. In this post, we examine how the Chaayos episode would have been treated under the draft Bill, with a view to understand how the law proposes to deal with the issue of consent and the possible penalties for breach of these provisions.

How is Chaayos classified?

To begin with, the Bill would consider Chaayos as a "data fiduciary" since it decides the means and purposes of processing of personal data. The customer would be a "data principal".

The data captured by the FRT system would constitute "biometric data" as it includes "sensitive personal data" ('SPD'). Due to the particular vulnerability that misuse of such types of data can result in, the Bill imposes certain additional obligations on entities that seek to use this category of personal data.

Further, Section 92 of the Bill empowers the government to notify certain categories of biometric data that entities are barred from processing altogether, unless specifically authorised or required to do so by a law. This would imply that while normally, biometric data such as images of one's face could indeed be processed by a company such as Chaayos, the government can prohibit such practices. The grounds on which such a decision will be based are however unclear from the bare text of the proposed law.

Proportionate obligations under the PDP Bill, 2019

In order to give individuals greater control over their personal data, the Bill grants data principals a number of rights and imposes concomitant obligations on data fiduciaries. However, in order to ensure that obligations on entities are proportionate to the risks involved and to ensure that entities are not overburdened by the law, the Bill imposes obligations in a graded manner.

Under Section 26, certain data fiduciaries can be deemed “significant data fiduciaries” based on factors such as the volume of data processed, the turnover of the fiduciary, the risk of harm, or the use of new technologies in the processing. These entities will then have to comply with certain additional obligations such as preparing data protection impact assessments, appointing a data protection officer, and ensuring annual audits by an independent data auditor.

On the other hand, Section 39 of the Bill excludes certain “small entities” from having to comply with the law, should they process personal data manually (for instance, through maintaining written records). Such entities will be notified by the proposed Data Protection Authority having regard to factors such as the turnover of the entity, the purpose of collecting the data and the volume of data being processed. Notified entities will not have to comply with a number of provisions in the law such as those pertaining to notice and data retention, user rights (of access, rectification and erasure, data portability and right to be forgotten), as well as the transparency and accountability measures (such as the need to put in place security safeguards or report data breaches).

In our example, given the use of biometric data and facial recognition technology, it is not inconceivable that Chaayos could be categorised as a “significant data fiduciary”. It would then have to comply with the additional obligations mentioned above. This implies that companies will have to make a reasoned decision about their data processing practices, particularly for functions that are not strictly related to their business. Should they choose to introduce a range of new but not strictly necessary features, they will have to take on the costs of complying with additional obligations. That said, Chaayos will not be able to claim the exemption under Section 39, as it is clearly using automated technology to carry out the processing.

How does consent work under PDP Bill, 2019?

The PDP Bill requires a data fiduciary to only process personal data if it has a valid ground to do so. The most important aspect of this is obtaining the consent of the data principal. Section 11 of the Bill requires the data fiduciary to ensure that it secures “explicit” consent of the data principal before or at the time of collecting SPD. The onus is on the entity concerned, which is Chaayos in our case, to prove it adequately secured consent.

But what does this entail? How does the law seek to ensure that the individual is properly informed and in control of their information?

How do these provisions work with the Chaayos hypothetical?

As per the Bill, in order for consent to be considered valid, it must be:

1. **Free**, that is, not induced by fraud, misrepresentation, coercion, undue influence or mistake. This implies that the data principal must not be forced or tricked into providing consent. She must be given a real choice about whether to provide the information or not. Thus, Chaayos will not be permitted to start recording the customer's image the moment she enters a store or picks up the tablet used for the FRT. The customer must first be given an option about whether to use the system or not.
2. **Informed**, that is, that the data principal must be provided the information listed in Section 7 of the Bill, that is, information pertaining to the purposes to which the data will be put to, the types of data being collected, information on how to withdraw consent, who the data will be shared with, etc. This information is to be provided in a clear and concise manner, that is reasonably comprehensible, and in multiple languages where necessary. This provision is important as it allows the data principal to understand the risks involved, and therefore make a rational choice about providing consent. In the context of SPD, the law also requires the data principal to be informed of any particularly harmful risks that they may be exposed to by allowing the processing of their data. In our hypothetical, Chaayos would have to provide the customer an easily accessible set of terms which provide her all the relevant information needed to decide whether to consent to the processing, as well as information regarding how to withdraw consent or make complaints to the company.
3. **Specific** consent given must relate specifically to the purpose of processing that is contemplated by the fiduciary. The consent clause must not be overly broad or ambiguous or encompass unconnected purposes. In the context of SPD, the data principal must be given granular choice, that is, the choice of making separate decisions regarding different categories of SPD that are to be collected and processed. Thus, Chaayos would have to provide information regarding the provision of the FRT system itself and the possible consequences stemming from using/not using the system. Their notice would also have to specify the types of information collected, who it would be shared with, the purposes it would be used for and so on. The challenge with this will be to ensure the notice contains all the relevant information without making it inaccessible to a common person. However, Chaayos could choose to use the model notices that the proposed Data Protection Authority will issue, thereby making it somewhat easier to comply with the law.
4. **Clear**: This means that the consent must be indicated through an affirmative action that is meaningful, given the context. In the context of SPD, the law requires express consent to be obtained, with specific additional "affirmative action" taken by the individual. There must be no doubt that the individual concerned wanted to consent to the processing of their SPD. Chaayos would then have to ensure that the customer specifically and ex-

pressly consents to the processing of their image — say by clicking on an empty check-box since mere silence or the use of pre-checked boxes will no longer be considered valid.

5. **Capable of being withdrawn:** This also involves ensuring that withdrawing consent should be comparable to the ease of giving consent. Thus, since the customer can give consent by ticking a box on a form, they should not have to send a physical letter to Chaayos requesting them stop processing the data. Additionally, it would be preferable if customer is given the option of sending an email to the company. The withdrawal of consent should also be followed by the deletion of her personal data that has been collected by the company, subject to any law in force.

Importantly, the data fiduciary cannot make the provision of any service dependent on the provision of personal data that is not necessary for the purpose.

How will this work in practice?

The draft Bill has introduced the concept of a “consent manager”, who is a data fiduciary tasked with enabling the data principals to manage their consent, through an interoperable platform. Thus, the Chaayos customer can write to Chaayos, either directly or to the consent manager, to exercise her rights of confirmation, access, correction, erasure, and data portability. The withdrawal of consent can also take place through the consent manager.

The idea behind a consent manager may be to reduce the incidence of “consent fatigue”, though how it will work in practice remains to be seen, and will largely be determined by the regulations that will be notified. Section 23(5) of the draft Bill states that the consent manager shall be registered with the DPA and be subject to various technical, operational, financial and other conditions, as may be specified by regulation.

What if you do not consent to the use of your image? Can Chaayos refuse to serve you tea altogether?

Under the draft Bill, Chaayos cannot outright refuse to serve you. The selling of tea itself is unconnected to the purpose of the processing of the facial image — which is to provide certain additional service features (such as repetition of orders, easier payments, etc.). Chaayos can, however, make access to these specific features dependent on the use of the FRT. They could therefore legitimately refuse to provide you the *convenience of choosing to repeat a previous order at one click*, but *cannot* refuse to serve you tea.

What if Chaayos refuses to follow the law?

The draft law seeks to ensure compliance by envisaging fairly stringent penalties. Data principals are empowered to make complaints to the company concerned, and if unaddressed can escalate them to the proposed Data Protection Authority

for redress. Further, the Authority can, on its own motion, investigate any untoward practices.

If subsequent to a hearing, Chaayos is found guilty of breach, it could be liable to pay a penalty extending to 15 crore or 4% of its global turnover in the preceding financial year. Further, it could be forced to pay compensation to a data principal who can demonstrate that she had suffered “harm” as a consequence of the illegal processing of her personal data.

Under the draft Bill, under Section 82, only the knowing or intentional re-identification of personal data, which has been de-identified by a data fiduciary/data processor, has been criminalised. The Bill departs from the Justice Srikrishna Committee version in three important aspects:

1. **It removes the offences of obtaining, transferring, or selling personal data and sensitive personal data contrary to the Act.** Under the 2018 version, if a customer’s biometric data had been collected by Chaayos with their express consent, but later, any person had knowingly/intentionally/recklessly disclosed or shared this data with a third party, that person could be punished with imprisonment up to three years. This is not the case under the present 2019 Bill.
2. **Even for the offence it retains, that is, re-identification, the 2019 Bill removes the standard of “reckless” as a basis for criminalising certain actions.** Suppose all the SPD collected by Chaayos has been anonymised by it (although whether data can truly be anonymised to prevent re-identification is questionable). If some person, without the consent of Chaayos, intentionally re-identifies the data, they are liable to be prosecuted and punished. However, if the re-identification happens unintentionally, recklessly, or negligently, that is, if the person is not aware about the possibility of re-identification if two data sets were combined, but should have known; and hence, they ignore the danger and go ahead and combine the data set, then even if it leads to re-identification, no one can be criminally prosecuted.
3. **Only the Data Protection Authority is permitted to initiate criminal action for the offence under Section 82.** This is unlike the previous version of the Bill. This provision under Section 83(2) is similar to Section 47 of the Aadhaar Act, which was struck down by the Supreme Court in the Aadhaar Judgment, and had to be amended pursuant to the Aadhaar Amendment Act, 2019.

Overall, while the draft law does put in place a number of measures to ensure that individuals are given greater control of their personal data, it remains to be seen whether a consent based regime — however improved it may be from contract law standards — will actually change data processing practices for the better. Will consumers actually seek to take control of their data, including by taking the additional time to read privacy policies and make rational choices? Will they be able to successfully take action against companies that violate the provisions of the law? Only time, and perhaps the Regulations that will be

notified by the Data Protection Authority, will tell.

*

Vrinda Bhandari is an advocate practising with the Delhi High Court, who works on issues concerning privacy, data, and digital rights.

Rishab Bailey is a fellow with the technology policy team at the National Institute of Public Finance and Policy, New Delhi. He has previously worked at a law firm, a software company, and with various civil society organisations on issues concerning technology policy and digital rights.

Edited by Aditi Agrawal

Regulatory governance under the PDP Bill: A powerful ship with an unchecked captain?

As the Joint Parliamentary Committee considers the Personal Data Protection Bill, 2019, MediaNama will publish a series of articles from legal experts focussing on the key aspects of the Bill and how they will affect users and companies. This is the second article in the series. Read our extensive coverage of the Bill here.

By Smriti Parsheera

“I prefer to sail in a bad ship with a good captain rather than sail in a good ship with a bad captain.”

— Mehmet Murat ildan

If the ship here is a metaphor for the rights and obligations offered by the draft Personal Data Protection Bill (PDP Bill) and the Data Protection Authority of India (DPA) as its captain, where does the current draft of the Bill leave us? Is it a good ship with a good captain or does it place the wheels of a powerful untested machine into the hands of an untrained and unchecked captain?

The preamble to the PDP Bill offers a precursor to the ambitious task that the Bill sets out for itself. It lists the various objectives of the law, which include specifying the usage and flow of personal data, creating organisational and technical measures for data processing, monitoring cross border data transfers and providing remedies against harmful processing. It then speaks of the role of the DPA as the agency responsible for giving effect to all of those purposes.

As per Section 41 of the PDP Bill, the DPA is to be set up as a body corporate, consisting of a Chairperson and up to six whole-time members. In adopting this structure, the Bill deliberately opts out of allowing any part-time members on the DPA's board. This is not in line with the practice that has been followed in the composition of many other statutory agencies. For instance, the Telecom Regulatory Authority of India can have up to two whole-time and two part-time members in addition to the Chair. By closing the possibility of having such part-time members, the Bill denies the DPA the opportunity to gain from the expertise of academics, researchers, practitioners and technical experts who could otherwise have injected independent ideas and critiques into its functioning.

While the draft does allow the DPA to engage consultants and experts to help it in the discharge of its functions (Section 48), this is very different from having independent voices in the management of the DPA itself. Further, the experience of other regulators shows that provisions of this nature are generally used for hiring entry-level researchers and consultants rather than those who might be in a position to drive policies at the top level.

A new concept that has been introduced in this Bill is that one of the members of the DPA has to be a person qualified in law. This is perhaps an attempt

to ensure the legitimacy and effectiveness of the DPA's adjudicatory functions, assuming that the legal member would be the one overseeing those activities.

Moving on to the DPA's selection process, all of the members are to be appointed based on the recommendations of an executive-led selection committee consisting of the Cabinet Secretary and the Secretaries in-charge of Legal Affairs and Electronics and Information Technology. This is a troubling departure from the draft that was proposed by the Justice Srikrishna Committee, which required that the selection committee should be headed by the Chief Justice of India or another judge of the Supreme Court. In addition, it was also to have another independent expert nominated by the judicial member.

Why is the constitution of the selection committee so relevant?

The success of the DPA, especially in the initial years when the foundational regulations and practices will be put in place, will depend to a large extent on the quality of its leadership. With an exclusively executive controlled selection process the chances are that the DPA will fall prey to the standard Indian practice of appointing former bureaucrats as the heads of regulatory agencies. This is already the case with the present banking, securities, insurance and telecom regulators in the country. While the persons selected in this manner may no doubt be competent individuals, the inherent flaw in such a system is that it perpetuates the hierarchies of the government set up into the functioning of what is supposed to be an independent regulatory body.

The DPA's independence from the government becomes particularly important given that it will not only regulate the private sector but also supervise the personal data processing of all government agencies. Bonhomie between the DPA's leadership and other government bodies could therefore result in weaker enforcement of the law. Let us examine this using an example.

Suppose an individual manages to discover an unencrypted database containing the personal details of all the beneficiaries of a public subsidies scheme. They report it to the concerned government department and the DPA. What is the DPA expected to do in such a situation?

The PDP Bill requires that every data fiduciary should implement necessary security safeguards like encryption, de-identification and measures to prevent unauthorised access (Section 24). Presumably, one of the likely reasons why the data could be accessed by a third party in this case was due to the department's failure to adopt appropriate security checks. The fact that the data was kept unencrypted makes it all the more vulnerable to being misused.

If such a situation of unauthorised or accidental disclosure of data leads to a compromise of its confidentiality, it amounts to a "data breach" (Section 2(29)). The department would therefore have to assess if the breach is likely to cause

any harm to the affected individuals. If so, it should immediately inform the DPA about the breach, its possible implications and any action taken to control the damage arising from it (Section 25). The DPA will then have to take a call on the best way to deal with the data breach, including determining whether the department should be compelled to inform the concerned beneficiaries of the scheme or the public at large about the breach.

In addition, the DPA will have to decide on what action it should take against the department for failing to secure the data in the first place. The range of orders that the DPA may pass for any such contravention of the law includes the issuance of a warning, directions to discontinue a violation of the law or temporary suspension of the fiduciary's activities (Section 54). In addition, the DPA can also impose a penalty of up to fifteen crores on the department for its failure to ensure appropriate security standards (Section 57(2)). The factors to be considered by the DPA while deciding on the levy of any penalty or payment of compensation to affected individuals include the nature and gravity of the violation, level of harm suffered and whether the violation was intentional or negligent in character (Sections 63(4) and 64(4)).

In the scenario described above, how might the DPA's actions be affected by the fact that the violator in question is a government agency? Would the risk of reputational damage to the department or its officials or any sort of political risks influence the DPA's decision on whether to go public about the breach? Further, since the department is performing a legitimate state function of delivering subsidies, is it practically possible for the DPA to place any restrictions on its data processing activities? A warning, reprimand or suggested remedial measures are perhaps the more likely interventions that we can expect in such cases.

Finally, when it comes to the potential imposition of a penalty, this decision is completely dependent on the initiation of a complaint by the DPA (Section 63(1)) followed by an adjudication process to be conducted by its officers. Given the composition and structure of the DPA one can expect that any penal action against the government would be reserved only for the most egregious of circumstances.

Suppose in the above example, the government entity had taken appropriate measures to de-identify the data that was leaked but the individual who found it intentionally used it to re-identify the beneficiaries of the scheme. What action may be taken by the DPA in such a case?

The individual's actions in the above scenario amount to the commission of an offence under Section 82 of the draft Bill, which is punishable with an imprisonment of up to three years and/or a fine of up to two lakh rupees. However, the PDP Bill bars courts from taking cognizance of any such offence, except in case of a complaint made by the DPA (Section 83(2)). The DPA will therefore have the discretion to decide whether to initiate any criminal action against the

individual.

It is curious to find that the PDP Bill chose to opt for this formulation despite its explicit rejection by the Supreme Court in the context of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (Aadhaar Act).

The original text under Section 47 of the Aadhaar Act contained a provision similar to the PDP Bill, which allowed only the Unique Identification Authority of India to initiate a complaint for any offence committed under that law. The Supreme Court, however, declared this to be unconstitutional, with the majority decision in the *Puttaswamy* case noting that:

“By restricting the initiation of the criminal process, the Aadhaar Act renders the penal machinery ineffective and sterile ... Such bar is unconstitutional as it forecloses legal remedy to affected individuals.”

This led to an amendment of the Aadhaar Act in 2019 to clarify that a complaint could also be initiated by an Aadhaar number holder or individual. It is necessary that a similar provision should also be included in the PDP Bill.

Transparency in DPA’s regulation-making process

The example above refers to the monitoring and enforcement functions of the DPA, in essence, its duties to ensure compliance with the provisions of the law. In addition to this, the DPA also has the power to frame subordinate legislation on many important aspects. Here, it is curious to find that the PDP Bill draws an unexplained distinction between the process to be followed in case of the framing the codes of practice for data fiduciaries and all other types of regulations. Examples of the codes of practice listed under the PDP Bill include the process for obtaining valid consent, data portability standards, anonymisation methods, etc. In all such cases the PDP Bill requires that the adoption of the codes has to be done in a transparent and consultative manner (Section 50(4)). There is, however, scope to further improve this provision by codifying the details of the process to be followed by the DPA to ensure careful deliberation by the DPA and effective participation from stakeholders.

On the other hand, when it comes to the framing of all other regulations (other than the codes of practice), the PDP Bill is completely silent in terms of requiring the DPA to follow a transparent and deliberative process. The reason for the inferior treatment for this category of regulations, which have the effect of law and can therefore bear significant consequences for data principles and fiduciaries, is not clear.

For instance, the Bill allows the manual processing of data by “small entities” to be exempted from certain requirements under the law (Section 39). While it does provide the suggested criteria for designating such entities, for instance based on their turnover and number of users, the actual classification is left to be done by the DPA through regulations. Another requirement under the Bill

is that significant data fiduciaries should undertake a data protection impact assessment under certain circumstances, and the DPA can specify the cases in which this exercise would be mandatory (Section 27). This decision also has to be made through regulations to be framed by the DPA.

In both these cases, the regulation-making process will not have to be subject to any consultation, debate or cost-benefit analysis. This sort of an opaque decision-making processes vests a tremendous amount of discretion in the hands of the DPA.

The same observations also hold true for the various situations where the law empowers the Central Government to take decisions “in consultation with the Authority”. Examples of this include the notification of additional categories of sensitive personal data under Section 51(1); declaration of certain social media intermediaries as significant data fiduciaries under Section 26(4); and issuance of directions for the provision of any anonymised personal data or non-personal data under Section 91(2). Unless such a requirement is built into the law, the DPA would not be required to follow a transparent, consultative process while rendering its advice to the government on these important aspects.

DPA's control over the innovation sandbox

The 2019 version of the Bill also introduces a new concept of a “sandbox”. It gives the DPA the authority to modify the application of certain provisions of the law for eligible entities that are engaged in “innovation in artificial intelligence, machine-learning or any other emerging technology in public interest”. The relaxations that may be provided in the sandbox include exclusions from the need for having a clear and specific purpose for data processing, collection only for a specific purpose and limited period of retention of the data (Section 40).

In order to be eligible for the sandbox an entity should have in place a suitable privacy by design policy that has been certified by the DPA (Section 22). This is an odd provision in that it requires the DPA to verify and certify the fiduciary's managerial and business practices, the technology being used by it and the transparency of its data processing. All of these are matters which would ordinarily have to be verified by the DPA only in ex-post facto circumstances, in case of an inquiry or adjudication proceedings.

The present formulation of the sandbox and privacy by design provisions gives rise to several concerns:

1. **Burden on DPA:** The requirement to certify the privacy by design policy of each entity that makes such a submission would cast a huge burden on the DPA. Given the large number of fiduciaries in the ecosystem this sort of prior certification does not seem to be the best use of the DPA's time and resources.
2. **Lack of clarity around the certification:** The implications and purpose of the certification are also unclear. If the objective is mainly to

make sure that any entity that seeks to enter into a sandbox has the basic processes in place, that could have been achieved through other mechanisms. For instance, the DPA could follow a case-by-case analysis only for those entities that seek to apply for the sandbox. Alternate requirements like self-certification or third-party audit of the relevant entities could also have been considered, along with suitable checks and balances.

3. **Ambiguous conditions:** The factors to be considered by the DPA while allowing entry into the sandbox include judging whether the activity being pursued by the fiduciary is in “public interest” and if it amounts to an “innovative use of technology”. The undefined nature of these terms vests ample discretion in the hands of the DPA in deciding which entities would be included or excluded from the sandbox.
4. **Lack of transparency in the regulation-making process:** The detailed process and additional criteria for applying for the sandbox as well as the privacy by design certification is left to be determined by the DPA through regulations. This circles back to the issue of lack of transparency and accountability requirements in the DPA’s regulation-making processes.

In summary, the PDP Bill grants many far reaching powers to the DPA. Most of the principles laid down in the draft law are to be supplemented by regulations and codes of practice to be adopted by the DPA. In addition, the DPA is also responsible for monitoring compliance with the law, providing redress to aggrieved individuals, monitoring technological developments and promoting awareness among stakeholders. While casting all of these diverse functions on the DPA, the Bill, however, fails to go far enough in terms of ensuring the independence and the accountability of the agency.

The lack of procedural safeguards in the draft Bill coupled with weak state capacity leaves us in a situation where even a well-intentioned captain might not be able to successfully steer this ship, let alone the havoc that may be caused by a rogue one.

*

Smriti Parsheera is a fellow with the technology policy team at the National Institute of Public Finance and Policy, New Delhi.

Edited by Aditi Agrawal

Personal Data Protection Bill, 2019: Considering data localisation and its effects on payments

As the Joint Parliamentary Committee considers the Personal Data Protection Bill, 2019, MediaNama will publish a series of articles from legal experts focussing on the key aspects of the Bill and how they will affect users and companies. This is the third article in the series. Read our extensive coverage of the Bill here.

By Nikhil Sud

This article has been written considering this scenario in light of the Personal Data Protection Bill, 2019:

An OTT platform offers services in India but uses an international payment gateway to process payments. Does the OTT platform need to be a part of a DPA-approved intra-group scheme? What about the payment gateway? How does the intra-group scheme requirement interact with the RBI's data localisation mandate?

Considering the scenario — a few impressions

(The following does not constitute legal advice.)

This scenario involves two types of data:

1. The payments data noted in the scenario and
2. Any other data that the OTT platform processes as part of its service offering.

However, this article — like the scenario — focuses on type (1). The Personal Data Protection (PDP) Bill's localisation provisions likely apply to this data for multiple reasons.

First, this data likely comprises “personal data” per the Bill’s definition of “personal data”. The definition, given its concerning breadth, would likely apply despite measures that the OTT platform or payment gateway may take to make it difficult to identify individuals from this data.

Note: If, however, this data is anonymised (per the Bill’s definition of “anonymisation” which requires, arguably impractically, “irreversible” anonymisation), then the Bill would consider the data “non-personal data,” potentially allowing the government to demand access to that data to help the government improve the delivery of government services. Complying with this demand may require some form of localisation, depending on the additional guidance the government is expected to release on non-personal data. Policymakers should have reserved the matter of “non-personal data” entirely for a separate proposal and consultation, in line with the separate committee established by MEITY to explore “non-personal data”. This is because non-personal data, by definition, does not

pertain to privacy (the core and impetus of the PDP Bill), and because its exact meaning and how exactly it should (and whether it can) be used without hampering innovation and competition are highly complex issues, meritng deep, thoughtful analysis and consultation before any legislative activity. Illustratively, India's draft e-commerce policy, published early last year, addressed non-personal data without thorough consultation, resulting in language that was confusing, inconsistent, and potentially detrimental to competition and innovation.

Second, this data likely comprises “sensitive personal data” under the Bill’s controversially broad definitions of “sensitive personal data” and “financial data.”

Note: Of course, the fact that (per the scenario) much of this data’s processing is likely conducted abroad by the international payment gateway likely does not protect that processing from the Bill’s localisation provisions. This is because that data was likely collected in India and had to be transferred abroad (which seems the sort of data for which the Bill’s localisation provisions are designed — Section 34, which articulates these provisions, is framed as discussing the “transfer” of data outside India), and because the non-Indian nature of the gateway likely does not shield it from the Bill’s obligations (see, for example, Section (2)(A)(c)(i)). If, however, this data was not collected in India (which seems unlikely), then it is unclear if any localisation requirements would exist. Section 2(A)(c)(i) suggests that the Bill would apply, implying that its localisation requirements would exist; however, the Bill’s localisation requirements appear to assume that the data (to which they apply) was collected in India (as noted above, the Bill – when addressing localisation – prescribes requirements for the “transfer” of data abroad).

Transferring this data abroad

Setting aside the aforementioned complexity and proceeding on the basis that this data was collected in India (and, as discussed above, this data comprises “sensitive personal data”), this data “may be transferred outside India, but ... shall continue to be stored in India” per the Bill. Policymakers should clarify the meaning of this language. It could mean that though the data can be transferred abroad temporarily for processing, it must be brought back to India and stored in India after the processing. It could alternatively mean (among potentially other things) that even if this data is transferred abroad, a copy of it must remain in India.

Either way, for the data to move abroad, the data principal must provide explicit consent, and certain other requirements must also be met per Section 34, which deals with the transfer of data abroad.

Using an intra-group scheme

One option, per Section 34, is for the transfer to occur through an intra-group scheme between the OTT platform and the payment gateway.

Note: Assuming that the OTT platform “determines [alone or in conjunction

with the payment gateway] the purpose and means of processing” the data, the OTT platform is likely the “data fiduciary” and the payment gateway is likely a “data processor” per the Bill. Both parties are thus subject to obligations in the Bill, but per Section 10 of the Bill, the data fiduciary is responsible for compliance with the Bill in relation to the processing it undertakes or the processing that others – such as data processors – undertake on its behalf.

The scheme between the OTT platform and the gateway would need approval from the Data Protection Authority (DPA). For approval, the DPA will likely require (among other things) that the scheme contain “effective protection of the rights of the data principal under this Act, including in relation to further transfer to any other person.” Policymakers should provide guidance on the precise meaning of this language. For example, what exactly constitutes “effective protection”? More fundamentally, requiring DPA-approved schemes is not ideal; it can strain the resources of the DPA, the data fiduciary, and the data processor, and foster uncertainty, potentially chilling data flow, investment, and innovation. Policymakers could instead consider incorporating into the Bill the principles articulated in the voluntary and widely embraced APEC Privacy framework and the APEC Cross Border Privacy Rules (CBPR) which seek to balance innovation with privacy.

Besides using an intra-group scheme, the platform has other options

It could attempt invoking the Bill’s Sections 34(1)(b) or 34(1)(c). Both would likely require engaging with the government and the DPA.

1. Under Section 34(1)(b), the government — in consultation with the DPA — could allow transferring this data abroad if it concludes that the data will be adequately protected in the destination country. However, it is unclear how the government will assess adequacy; policymakers should make this clear and consult all stakeholders when deciding how the government will assess adequacy. Section 34(1)(b) also requires that the transfer “shall not prejudicially affect the enforcement of relevant laws”. This language too calls for clarity, and risks a broad interpretation that could stifle data flow, given the strikingly wide powers the bill elsewhere provides the government to collect and process personal data.
2. Under Section 34(1)(c) of the Bill, the DPA could allow the “transfer of any sensitive personal data...for any specific purpose.” The seemingly welcoming language of this provision — signaling an openness to data flow — is at least partly offset by the lack of clarity on how the DPA will make this assessment. The assessment should be conducted reasonably and transparently, and all stakeholders including industry should be consulted when policymakers decide how the DPA will conduct this assessment.

Interplay between RBI’s localisation mandate and PDP Bill

The interplay creates the risk of a fragmented landscape with potentially unclear and conflicting obligations, stunting innovation and investment. This risk is

exacerbated by the confusion surrounding the RBI's mandate, alleviated only partially by the guidance (FAQs) that the RBI released in June 2019, more than a year after it issued the mandate in April 2018.

Broadly, while all of the payments data mentioned in the scenario likely falls under the scope of the Bill, some of that data (though not necessarily all of it) may *also* fall under the scope of the RBI's mandate, depending on the exact nature of the data processed by the gateway, and on the categories of data articulated in the RBI's localisation guidance. For the data to which both sets of rules apply, it is unclear which set trumps the other. The PDP Bill, designed as a cross-sector bill, should arguably trump the RBI's rules (especially given Section 96 of the Bill, discussing the overriding effect of the Bill).

However, the PDP Bill frequently recognizes the importance of sectoral regulators in shaping data protection rules, potentially signaling deference to them. Additionally, policymakers in their public comments have generally signaled some deference to sectoral regulators. Further, in situations where the RBI's rules exceed the PDP Bill's rules, policymakers may construe the two sets of rules not as inconsistent but as complementary – they may interpret the PDP Bill as setting the baseline, and the RBI as adding requirements beyond the baseline, thereby allowing the RBI's rules to apply.

Separately, at least three additional sources of uncertainty and complexity exist:

First, the PDP Bill requires “critical personal data” to be processed only in India (subject to certain exceptions) but does not define “critical personal data.” It defers to the government for the definition. If the government defines “critical personal data” to include some forms of financial data, that could alter the assessment above, and impose heightened obligations. Relatedly, if the government defines “critical personal data” in consultation with sectoral regulators such as the RBI, the definition could support the RBI's localisation goals (which appear to exceed the PDP Bill's localisation goals), impacting the assessment above regarding the interplay between the PDP Bill and the RBI's mandate.

Second, the PDP Bill empowers the DPA and the government to issue substantial additional guidance on a variety of matters including localisation. Until this guidance is issued, uncertainty will persist. There is also a risk that this guidance is overly stringent. Though the Bill commendably requires every rule and regulation made under it to be tabled in Parliament, the government and the DPA should consult all stakeholders, including industry, before developing any such additional guidance.

Third, policymakers' views on these issues frequently evolve and this evolution is not always reflected — or reflected in a timely manner — in the written materials produced by policymakers. Further, and relatedly, some policymakers sometimes signal one view on the meaning of a policy, while others signal a different view on the same policy, neither of which is reflected in written materials.

This all perhaps stems from the complexity of these issues, but policymakers should react to that complexity differently: they should adopt thorough, transparent, well-organized, collaborative, and numerous wide-ranging consultations, fueling a coherent and clearly articulated policy. Otherwise, industry is forced to make critically important investment decisions based on information that is sparse, ambiguous, and unreliable (as it may not reflect policymakers' latest thinking, or it may reflect one policymaker's thinking but not another's). This all risks deterring investment and innovation, and ultimately hurting consumers.

In conclusion

The Bill's data localisation requirements would likely apply to the data in this scenario. Complying with these requirements can prove challenging, forcing the platform to navigate complex and onerous rules. Additionally, the platform faces significant uncertainty, stemming from the Bill's ambiguous language, the unclear interplay between the Bill and the RBI's localisation mandate, and the wide rule-making powers the Bill provides to the government and the DPA. These challenges could hinder the platform's ability to invest in India and innovate for Indian consumers. This is particularly concerning because the Bill's and the RBI's data localisation requirements may not materially bolster data security; are unnecessary for law enforcement; and risk creating a starkly uneven playing field between Indian and international players (though likely hurting Indian players much more than policymakers may anticipate).

*

Nikhil Sud serves as Regulatory Affairs Specialist at the Albright Stonebridge Group. He is a lawyer by training and specialises in legal and policy issues relating to technology.

Edited by Trisha Jalan

Personal Data Protection Bill, 2019: Looking at social media intermediaries and significant data fiduciaries

As the Joint Parliamentary Committee considers the Personal Data Protection Bill, 2019, MediaNama will publish a series of articles from legal experts focussing on the key aspects of the Bill and how they will affect users and companies. This is the fourth article in the series. Read our extensive coverage of the Bill here.

By Sajan Poovayya and Priyadarshi Banerjee

The story of internet penetration in India coinciding with the boom in mobile telephony implies that most users in India access internet only through smartphones. While no doubt, this may facilitate access to the internet at an unprecedented scale, it also calls for attention to the typical user behaviour whereby consumers unwittingly agree to submit their personal information to social media apps and other similar platforms, for free use of their services. This pattern of behaviour and its global exploitation have come to the fore in recent times raising concerns in terms of *inter alia* a data principal's privacy and larger societal concerns in terms of micro-targeting of users, utilising personal data shared on social media platforms and its effects on electoral democracy, etc.

Much of the public attention that the subject of data protection had received in this country stemmed from concerns of unauthorised and opaque sharing of personal data by data fiduciaries with third parties, without the knowledge or consent of the data principal. Further, recent controversies about distortion of electoral views through means of unauthorised and clandestine sharing and processing of personal data necessitates an analysis to see how the Personal Data Protection Bill, 2019 (the "2019 Bill"), measures up to such recent challenges.

Sharing of personal data by social media Intermediaries

The proposed law seeks to safeguard the personal data of users (or data principals) by creating a tiered regime of informed consent for collection and processing of personal data, in a bid to reduce the opacity in data flow. The legislative idea seems to be to put the data principal in the driving seat and guarantee her a degree of autonomy and control over her own personal data. Before embarking on examining whether the 2019 Bill is equipped to deal with a situation akin to the Cambridge Analytica fiasco, consider the following:

1. A class of intermediaries under the proposed legislation are classified as 'social media intermediaries' which are intermediaries who primarily and solely enable online interaction between two or more users and allow them to create, upload, share, disseminate, modify or access information using its services;

2. A subset of personal data is separately defined as ‘sensitive personal data’ [Section 3(36)] which is an enumerated class consisting of data relating to financial information, health, sexual privacy, caste/tribe status, religious or political belief or affiliation. Such sensitive personal data is subject to a heightened level of protection, safeguards or restrictions in terms of regulations which may be subsequently formulated by the Data Protection Authority of India, created under this statute; and
3. Under Section 26 of the 2019 Bill, certain thresholds in terms of volume of personal data processed, the sensitivity of personal data processed, risk of harm, etc., are specified, upon satisfaction of which, the Data Protection Authority may notify a data fiduciary as a ‘significant data fiduciary’. The 2019 Bill further mandates that the Central Government ‘shall’ notify any social media intermediary as a significant data fiduciary if its actions have, or are likely to have a significant impact on electoral democracy, etc. Therefore, subject to any future notification by the Central Government, major social media intermediaries are as such liable to be notified as significant data fiduciaries which must comply with specific obligations under the proposed legislation.

How does the proposed law tackle the sharing of personal data by a social media intermediary with downstream data processors? Can a social media intermediary share personal data with a research company, which in turn may share it with a political party that uses it to micro-target voters?

Under the 2019 Bill, a data fiduciary (which would include a social media intermediary) is obligated to obtain consent for collection of data under Section 7, and consent for processing under Section 11. While seeking consent (by providing notice to a data principal at the time of collection of personal data) under Section 7, a data fiduciary must state the purposes for which the personal data is to be processed [Section 7(1)(a)], and inform a data principal about the individuals or entities including other data fiduciaries or data processors with whom such personal data may be shared [Section 7(1)(g)]. In this context, under Section 11(3), explicit consent is required for processing any sensitive personal data. The ‘religious or political belief or affiliation’ of a data principal is defined as sensitive personal data under Section 3(36)(xi) of the 2019 Bill.

Therefore, opaque unilateral sharing of personal data without intimation and consent of the data principal is ruled out under the proposed law. A data principal must be made aware of sharing of any personal/sensitive personal data with a third party through a notice under Section 7(1)(g).

Now, the obligations on any such third-party recipient of personal data and what activities it may undertake thereon are governed by the provisions of Section 31 of the 2019 Bill. Under Section 31(1), the data fiduciary (including a social media intermediary) must enter into a contract with any data processor to engage it for processing personal data. Under Section 31(3), such data processor

who receives personal data under a contract from a data fiduciary may only process such data in accordance with the instructions of the data fiduciary and is further prohibited from sub-contracting with another data processor under Section 31(2) unless the principal data fiduciary has explicitly permitted so in its contract with the data processor. Also, the data processor receiving personal data from a data fiduciary under Section 31 is obligated to treat such data as confidential.

Therefore, under the scheme of the proposed law, the data fiduciary at all times is in fiduciary control over the personal data and **no processing is permissible by a downstream data processor unless so explicitly permitted** under Section 31(2).

This, read with the data fiduciary's obligation to notify the data principal at the time of collection about the entities with whom personal data may be shared, implies that the data principal shall be transparently aware of the fate of any personal data which it reposes with such a data fiduciary.

The legal architecture as proposed in the 2019 Bill does not in essence prohibit the sharing of data by social media intermediaries with third parties. The proposed law requires that the user be furnished with notice of the possibility of such usage while her data was collected or subsequently processed. If the processing is that of sensitive personal data, then a specific consent is required from the data principal. Although it may seem, that a prohibitory framework (in terms of preventing sharing of personal data to third parties altogether) would have better served the interest of data principals, the proposed law seeks to create a consent-based framework which averts the crippling effect an all-or-none prohibitory framework may have had on the digital economy. The law seeks to strike a balance between the rights of the data principal and the business efficiencies which big data processing ushers in.

Remedies available to a data principal for breach of obligations

In light of the above, if a downstream data processor or data fiduciary unauthorisedly shares personal data with any other entity, it will fall foul of the proposed law, and an affected data principal may seek redressal under the provisions of Section 32. Redress under Section 32 may be sought from the data fiduciary itself, whereas under Section 32(4), if the data principal is dissatisfied with the response from a data fiduciary, she may file a complaint with the Data Protection Authority.

Further, an affected data principal may also invoke the jurisdiction of the Data Protection Authority under Section 53 for appropriate redress in case of any unauthorised sharing of data, seeking an inquiry by the Authority against the data fiduciary for conducting itself in a manner which is detrimental to the interest of data principals or for contravening the provisions of the law. Additionally, under Section 53, the Data Protection Authority has the power to *suo*

moto inquire into any activities of the data fiduciary if it has reasonable grounds to believe that certain processing of personal data is in contravention of the law or detrimentally affects the interest of the data principal.

In case of unauthorised profiling or micro-targeting of data principals which is in violation of the scheme as delineated above, leading to electoral distortions, even the Election Commission may initiate the process of inquiry by making a complaint to the Data Protection Authority as Section 53 does not stipulate any restrictions as regards who may initiate such a complaint. A recalcitrant data fiduciary or a data processor would be liable for compensation under Section 64.

Deterrent principle and its glaring omission

It is curious that the 2019 Bill deletes two significant provisions from its previous version as were proposed by the Justice B.N. Srikrishna Committee along with its 2018 version of the Bill. Two provisions from the older draft (Sections 90 and 91 of the 2018 Bill) — which had explicitly made obtaining, transferring or selling of personal data/sensitive personal data contrary to the provisions of the 2018 Bill an offence, — are now omitted. Inasmuch as the Justice Srikrishna Committee had adopted the deterrence principle as a necessary postulate for data protection, this glaring omission is a major departure therefrom.

The 2019 Bill falls seriously short of emancipating a data principal in terms of remedies afforded under it, when it proposes a truncated chapter on offences and simultaneously requires that no court shall take cognizance of any offence under this law unless the complaint in that regard is made by the Authority. The requirement to route the criminal process through the Data Protection Authority, in a manner, robs the data principal's agency to protect her personal data, which too, is a serious dilution of the deterrence principle adopted by the Justice Srikrishna Committee.

How does the proposed law deal with a political party that uses the data collected through its app to micro-target voters?

In connection with the data sharing fiasco surrounding Facebook and Cambridge Analytica, it is imperative to also consider the possibility of political parties themselves collecting data directly through some mobile applications for the purpose of micro-targeting voters. Possibly, surreptitiously. While it is possible that an application is facially innocuous (such as a meme-generator, a game, a pop quiz, etc.), the data collected in the process of using it may have a far reaching impact on the informational autonomy of a data principal. For instance, location data, cookies saved on a browser, search history, may, when aggregated or combined, create a profile of an individual for the purposes of micro-targeting.

Micro-targeting is a form of online targeted advertising which analyses personal data to identify the interests of a specific audience or individual in order to

influence their actions. It may be used to offer a personalised message to an individual or audience using an online service such as social media. It may determine what and how relevant content is delivered to an individual online and is sometimes used to market goods or services *and* for political marketing. For example, if you express an interest in a certain political party or ideology on a social network , personalised advertisements related to that party or ideology may be displayed to you; or, a political party may target propaganda material towards a data subject once it is aware of a particular political inclination of hers. There have been serious concerns of electoral manipulation through such means, the primary objection being that the data principal may not be even aware that she is being targeted.

Under the 2019 Bill, inasmuch as such a political party is collecting personal data of voters, it would be a data fiduciary under the 2019 Bill, as proposed. *Stricto sensu*, under the provisions of the proposed law, since political belief or affiliation is a sensitive personal data, such a data fiduciary (which in the present example is a political party) may also be notified by the Data Protection Authority as a ‘significant data fiduciary’ under Section 26 of the 2019 Bill. Therefore, such political party, being a data fiduciary, shall be required to issue notice of information (under Section 7) to the data principal at the time of collection of personal data specifying *inter alia*, the purposes for which such data may be processed. Also, under Section 11, the political party would need to obtain consent for processing the same from the data principal.

However, the status of a ‘significant data fiduciary’ is dependent on the affirmative act of notifying one as such, by the Data Protection Authority. Inasmuch as the appointment of the members of that Authority is at the hands of the Executive Government, its impartiality must be zealously maintained. In this regard, the legislative proposal of the Justice Srikrishna Committee was far-sighted when it proposed a judicial member (the Chief Justice of India or her nominee) be in the selection committee to ensure transparency and fairness in such appointment. However, the 2019 Bill seeks to constitute the selection committee solely with bureaucrats as its members.

Therefore, while in the minimum **such a political party has to comply with the requirements of informed consent for collection and processing of data under Sections 7 and 11 of the 2019 Bill, which itself provides a degree of safeguard to a data principal, such a political party may also be required to adhere to the additional obligations of a significant data fiduciary, if they are notified as such.** Once more, the legislative proposal seeks to usher in a regime of informed consent to provide a degree of informational autonomy to a data principal, which hitherto had been completely absent.

Conclusion

The development of a legal regime for data protection in India is presently in its nascentcy. Thus, it is fairly early to undertake a complete analysis of the data protection regime that is sought to be set up under the 2019 Bill. The Bill itself has multiple creases to be pressed out, some of which have been highlighted above. Additionally, contours of much of the protections are to be laid down through regulations once the law is operationalised. It is only when the Data Protection Authority is set up under the enacted statute that it shall commence the process of formulating Codes of Practices as required under the law. Therefore, weighing the efficacy of the entire process at present shall be no better than a soothsayer's chant. However, a robust framework has indeed been formulated after a herculean effort from both the Executive Government and the civil society participants in the process, which it is expected shall only be strengthened through parliamentary debate as this new regime is legislated.

*

Sajan Poovayya is a Senior Advocate practising in the Supreme Court of India. He has a vast experience in technology laws and regularly appears before various judicial fora on issues pertaining to technology and its interface with domestic legal obligations, both statutory and constitutional.

Priyadarshi Banerjee is an advocate practicing before the courts in Delhi, and has represented multiple social media companies in myriad litigation revolving around issues of privacy, intermediary liability and digital rights.

Edited by Aditi Agrawal

Personal Data Protection Bill, 2019: Protecting children's data online

As the Joint Parliamentary Committee considers the Personal Data Protection Bill, 2019, MediaNama will publish a series of articles from legal experts focussing on the key aspects of the Bill and how they will affect users and companies. This is the fifth article in the series. Read our extensive coverage of the Bill here.

By Smitha Krishna Prasad

Decades after the first data protection laws were implemented, we still continue to struggle with some of the basics of personal data protection — how should personal data be defined? Corollary to this, is the question of whether some personal data matters more than others.

Many privacy scholars now agree that the relevance and sensitivity of personal data should be determined by context. The idea is to protect individuals or groups of individuals in contexts where certain personal information makes them more vulnerable. Implementing this kind of protection under the law however, has not been as easy given how often ‘context’ and therefore sensitivity changes. The compromise that many lawmakers have found seems to be the categorisation of personal data and sensitive personal data – all data is to be protected, but certain types of data are sensitive irrespective of context and require increased protection. The brand new Indian Personal Data Protection Bill, 2019 (PDP Bill), also uses this approach, and lists out a number of categories of data as ‘sensitive personal data’.

While it is debatable whether sensitive personal data should be listed out, or a more dynamic approach is better — one of the few areas where there is consensus that additional protections are required irrespective of context, is in the case of personal information of children.

In this article, we look at what the PDP bill says about collection and processing of children’s personal data, what this actually means in practice, and how this stacks up against global or best practices.

Chapter IV of the PDP Bill deals with the personal data and sensitive personal data of children. It provides for a broad requirement that data fiduciaries must process personal data of children in a manner that protects the child’s rights, and is in the best interests of the child [Section 16(1)]. The rest of the chapter can be divided into two sections – the first, the provisions that go into when and how consent should be provided for the processing of such data, and who can provide such consent. The second issue this chapter focuses on is specific types of processing that will not be permitted in relation to children’s personal data.

The PDP Bill considers any person below the age of 18 a child, in line with Indian laws on the age of majority, which require a person to be 18 years of age

to enter contracts, vote etc. In this context, it is not surprising that one of the areas of focus in the PDP Bill's discussion on children and children's rights in the context of personal information is the issue of consent, that is, a contract between the data fiduciary and the person providing the consent.

What happens when children want to access online services?

First, the data fiduciary must verify the age of the child, and ensure that consent is obtained from the parent or guardian. The PDP Bill itself does not go into detail on how this is to be done — except that there will be regulations on how age verification is to be undertaken. In prescribing these age verification mechanisms, a number of criteria will be taken into consideration, including: the volume of personal data processed; how much of that personal data is likely to be that of a child; and whether it is possible that there will be any harm to the child from the processing of such personal data. Regulations will also classify data fiduciaries that operate commercial websites or online services directed at children, or process large volumes of personal data of children, to be 'guardian data fiduciaries'.

How will the PDP Bill affect apps like PUBG?

At this stage, while we will have to wait to see what the regulations look like, it is likely that services popular with younger age groups, will at least need to implement age verification mechanisms, if not act as guardian data fiduciaries. A good example here would be gaming apps — these are sometimes targeted specifically at children, but many of the more popular apps are widely used by children and adults alike. A risk of harm to children using these services also may exist, leading to the classification of such service providers as guardian data fiduciaries.

While in the past we have seen some extreme reactions to such services, such as the recent ban on PUBG, a gaming app that is popular globally, and popular specifically among children, might need to tweak some services under the new PDP Bill. First, age verification and consent mechanisms will need to be modified. The age of consent specifically for online services is higher in India than in many other jurisdictions – the US and the UK for instance allow children between the ages of 13 and 18 to provide consent for some services, often depending on the competence of the child to consent. However, India doesn't seem to be adopting this system of differentiated ages of consent, except in the case of data fiduciaries providing counselling or child protection services to a child, in which case no consent is required from the parent or guardian.

The PDP Bill calls for a consent manager system to be implemented, in order to battle some of the common problems we see with the informed consent system. It may be worthwhile to look at whether this can be used as a specific solution in the case of children's consent as well. However, given that there is little

information on what the role of consent managers will be, or how age verification systems will be implemented, we may need to wait until the data protection authority starts discussing regulations to engage more on this subject.

What can be effective age-gating mechanisms?

The kind of age verification system that needs to be adopted, will be discussed in more detail in the regulations. Implementing effective age verification systems is an ongoing problem, given that some of the simple age verification systems are often easy to circumvent. The same case can also be made for systems in place to obtain the consent of the parent or guardian, once it is established that the personal data of a child is being collected.

A popular solution for this purpose is to implement knowledge-based tests. For instance, an age verification system that relies on arithmetic tests, could in theory verify the age of the person consenting, if there is an expectation that children will not be able to make such calculations – but this may not be the case for older children. However, more extensive knowledge-based tests often end up collecting more personal data than required – it is important to keep in mind that data protection principles need to be applied to this testing system itself.

What will happen if a guardian data fiduciary defaults on its responsibilities?

The second requirement under Chapter IV of the PDP Bill is applicable specifically to ‘guardian data fiduciaries’ – these data fiduciaries are not permitted to engage in profiling, tracking, behavioural monitoring of children or direct targeted advertising at children. They are also barred from undertaking any other activities that may cause significant harm to a child. This provision is likely meant to address situations like the recent case in the US, where Google/YouTube was fined USD 170 million for knowingly profiting from the use of personal data of children by directing targeted advertising at them. Similar to the consent requirements, an exception may be made (in the regulations) for data fiduciaries that offer counselling or child protection services.

Under the PDP Bill, any violation of the provisions of Chapter IV could result in a penalty up to INR 15 crore or 4% of the worldwide turnover of the data fiduciary for the preceding financial year (whichever is higher).

Is Chapter IV of the PDP Bill enough?

As discussed above, it is important that children have additional protections against the processing of their personal data, especially where such processing goes against their interest. To this end, the two broad purposes of Chapter IV of the PDP Bill — (i) ensuring that age verification mechanisms are in place, and

(ii) barring the profiling and tracking of children, the monitoring of children's behaviour, and targeting of advertisement to children — are commendable.

However, a few issues jump out immediately on the reading of these provisions. Some may be fixed by restructuring the provisions of the PDP Bill, but others possibly require a more thorough understanding of children's rights.

1. The first issue, is the idea of guardian data fiduciaries — the purpose for this classification appears to be to identify those data fiduciaries that are more likely to be processing children's personal data, resulting in harm to such children. However, the concept of guardian data fiduciaries is not really put to use beyond such classification. They have no additional obligations, other than the bar on profiling, tracking and monitoring of children's data, and targeting of advertising towards children, and other processing that may cause significant harm to children. It is not clear here why this bar is limited to guardian data fiduciaries — are those data fiduciaries that don't meet this threshold then allowed to engage in these activities that may result in significant harm to children?
 - It may be more useful to equate guardian data fiduciaries to significant data fiduciaries under the PDP Bill — undertaking some of the additional compliances applicable to significant data fiduciaries, such as data protection impact assessments may help identify harms to children, and then ways to protect them, better.
2. Second, the issue of differentiated ages of consent and the definition of what causes harm to children. With children of all ages using technology, and particularly online services, it is important to acknowledge that there is a sliding scale of sorts when it comes to harms to different age groups of children. This has been recognised by the National Commission for Protection of Children's Rights, which provides separate guidelines to 'older children' in its guide to online safety of children. It is important in this context, to look at children's data protection under the PDP Bill, from the larger lens of children's safety, as well as the agency and rights of children. For instance, it is important that the consent of a guardian or parent is obtained before a 10-year-old is able to access an online service, and provide personal data to the data fiduciary. However, there may be different concerns at play in protecting a 17-year-old, who may require privacy protections not only from the data fiduciary, but parents and guardians as well. While the exception for counselling and child protective services is useful in this context, practical concerns regarding the accessibility of such services and the relevance of harm in these contexts need to be accounted for.
3. Third, the absence of sensitive personal data in the discussion of children's data. Although the title to chapter IV indicates that it addresses sensitive personal data of children, Clause 16 itself has no mention of sensitive personal data. There will undoubtedly be situations where the sensitive personal data of children will need to be processed by a data fiduciary. It is important that this is accounted for and addressed under the law.

*

Smitha Krishna Prasad is Associate Director at the Centre for Communication Governance, National Law University Delhi.

Edited by Aditi Agrawal

Personal Data Protection Bill, 2019: Looking at use of video recordings, facial recognition software and drones by police

As the Joint Parliamentary Committee considers the Personal Data Protection Bill, 2019, MediaNama will publish a series of articles from legal experts focussing on the key aspects of the Bill and how they will affect users and companies. This is the sixth article in the series. Read our extensive coverage of the Bill here.

By Vaneesha Jain

In *Puttaswamy*, the Hon'ble Supreme Court of India gave a resounding recognition to the Fundamental Right to Privacy under the Indian Constitution, and stressed the urgent need for an overarching data protection law to protect this right to privacy. The Personal Data Protection Bill, 2019, which is applicable to both Government as well as private entities, does this by putting in place a framework for notice and consent to the data principal before their data is collected or processed, imposing obligations for data protection on the data fiduciary and data processor, and setting up a mechanism for regulation and penalties for contravention.

The PDP Bill lays a strong emphasis on the obligation of any entity processing personal data to do so only for the purpose consented to by the data principal or which is incidental to or connected with such purpose. However, it also provides for certain deviations from this rule mandating prior informed consent in all cases, and these are the ‘Exception’ situations where personal data may be processed *without* obtaining prior consent — such as, when personal data must be processed in order to comply with an order or judgment of any Court or Tribunal in India.

The Bill also provides for ‘Exemptions’, wherein certain provisions of the Bill (extending beyond the ‘consent’ provisions alone) have no applicability in the situations provided as exempted. The exempted situations would play out as if there were no data protection law in place at all. Given that the need for an overarching data protection law to uphold the fundamental right to privacy was so strongly emphasised by the Hon'ble Supreme Court in *Puttaswamy*, the ‘Exemptions’ chapter should ideally be narrowly tailored to suit very specific situations that merit the abandonment of the protective cover of this law. However, on examination, we see that this is not so. Instead, in addition to providing for specific scenarios for exemption, the PDP Bill also provides some extremely broad exemptions, especially in favour of the Government.

What situations are ‘exempted’ from the application of the PDP Bill?

1. Specific situations: The protective cover of the core provisions of the Bill, which impose obligations on data fiduciaries, mandate stringent requirements of consent, ensure data principal rights, transparency and accountability measures and provide for protections while transferring personal data outside India, has been removed in specific situations, such as where personal data is processed in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of any existing law.

2. Blanket exemption: In addition, there is a blanket exemption which can apply *at the discretion* of the Central Government. This broader exemption power allows the Central Government to remove any or *all* of the protections provided by the data law, to the processing, by a government agency, of *any* personal data that it may decide. It can do so by exempting the application of this law to any agency of the Government. Further, there is nothing in the law that would prevent the Central Government from adding to the list of exempted agencies, from time to time. The exercise of this power is conditioned upon the Central Government being satisfied that it is expedient to do so

1. in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order; or
2. 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.

Could this blanket exemption be used to allow the police to record protesters and use the information to arrest them?

Yes. The police, as a Government agency, could be exempted from the application of the data protection law by the Central Government, under the blanket exemption, by stating that the recording of protestors and subsequent arrests are being done in the interest of ‘public order’.

In addition, if the protestors are seen as threatening to commit any act of violence punishable by law, then the recording of their personal data may be exempted from the procedural requirements of the data protection law, under the specific exemption relating to prevention, detection, investigation and prosecution of any offence or any other contravention of any law.

Typically, under these exemptions, it would be possible for the police to use handheld devices to record protestors in an Indian city, process the footage through a facial recognition software, cross-reference the results from the software on a national database of citizens (the Aadhaar database, the NPR and the NRC are all such databases) to find their personal details such as phone numbers and addresses and arrest them from their homes. While challenges to such arrest would exist by claiming democratic freedoms, the PDP Bill itself may not provide any recourse.

In fact, reports have already surfaced confirming that the Delhi Police has started using Automated Facial Recognition Software (AFRS) on footage filmed from protest venues.

Abroad, in countries such as Hong Kong and the United States, the threat of technology-based surveillance during protests has been widely recognised and circumvented by using face-masks to prevent the collection of facial recognition data — and governments have responded by introducing ‘mask bans’. Such mask bans have been challenged as being unconstitutional in those countries, with some success. As the intensity of protests and anti-protest measures increase, it is highly likely that these issues will crop up in the Indian context as well.

Interestingly, if AFRS is considered to be a ‘new technology’ under the PDP Bill, then its continued use by the police might necessitate them being notified as ‘significant data fiduciaries’ under the Bill, with additional obligations such as registration with the Data Protection Authority.

The PDP Bill also categorically prohibits the processing of any sensitive personal data such as biometric data (which would be implicated by the use of AFRS) by a significant data fiduciary using new technologies, without first undertaking a data protection impact assessment, which must be reviewed by a data protection officer and submitted to the Data Protection Authority along with the review, and any subsequent directions/conditions imposed by the Authority for the use of such technology must be complied with.

Of course, these protective provisions, designed to further secure citizens against invasions of privacy using new technologies, may also be made inapplicable to a Government agency such as the police via a direction by the Central Government, if such a direction can be justified under one of the conditions for application of the blanket exemption provision.

Would the PDP Bill allow the sharing of drone-recorded information at a political rally for purposes of propaganda?

Assuming that the drones are used after complying with the extant domestic regulations for the use of drones in India, it may still have major implications for data privacy. In fact, in a recommendation for legislation around the use of drones, the Hungarian Data Protection Authority has emphasised that data processing with drone-mounted accessories has data protection implications. This is because even the proper use of drones can be very invasive into the privacy of people due to the ability and effect of the tool to collect data about everything that is in its field of vision, which is, compared to the use of similar technologies, unusually wide and can be changed very quickly.

The ‘footage’ recorded/collected by drones installed with cameras or other equipment to monitor or people would be ‘personal data’ within the meaning of the PDP Bill 2019 since the persons would be ‘directly identifiable’ with the footage recorded. It would further constitute ‘sensitive personal data’ as well: specifically, given the easy ability to process the drone-recorded footage on fa-

cial recognition software, the drone-recorded footage may constitute ‘biometric data’; further, such footage recorded at a rally would also reveal ‘political belief or affiliation’ of a person, and can also be processed to further reveal religious belief, sexual orientation, transgender status, intersex status, caste or tribe, etc. Such categories of data are protected as sensitive personal data under the PDP Bill.

Recording of such data using drones, would constitute ‘processing’ as defined under the PDP Bill.

Now, the PDP Bill clearly provides that in case of processing of any sensitive personal data, the consent of the data principal must be explicitly obtained. ‘Explicit consent’ is the highest threshold for consent, and requires that in addition to the consent being free, informed, clear, specific and capable of being withdrawn, it must be obtained *after* informing the data principal the purpose of processing which is likely to cause significant harm, in clear terms without recourse to inference from conduct in a context and after giving her the choice of separately consenting to the use of different categories of sensitive personal data.

It would be practically impossible to meet this high threshold of obtaining ‘explicit consent’ from the people at the rally before recording them with drones. **Therefore, in view of the above, the police using drones to collect footage of people at a rally and then providing it to political parties for propaganda will be impermissible under the Bill.**

Thus, if the police still goes ahead and use drones to collect such data of people and provide it to political parties for purposes of political propaganda, they would attract penal liability under the PDP Bill, upto INR 15 crore.

Notably, when footage is recorded at a rally for purposes of use in spreading political propaganda/electoral campaigning, this is not exempted under the PDP Bill. This is because use of personal data/sensitive personal data for political propaganda cannot be legitimately justified as fulfilling any of the conditionalities required to trigger the exemption provisions — either the blanket provision as well as the specific exemptions. This is when the data protection provisions of the PDP Bill should kick into place to protect the privacy of individuals.

However, we cannot ignore the fact that the use of drones to capture footage during rallies and demonstrations is becoming increasingly normalised. In fact, in December 2019, there was a direction from the Madras High Court to the Police, as an interim measure, to videograph the entire area in which permission to carry out a demonstration, was sought — with specific permission for the use of drones, in order to identify leaders and hold them individually liable. The PDP Bill provides a specific exception to the need to obtain consent, when processing of personal data is done for compliance of any order of any Court in India.

Conclusion

In the first instance, the PDP Bill prohibits the recording of footage of protestors at demonstrations and rallies (given that the nature of recorded information constitutes personal data/sensitive personal data) without obtaining the highest threshold of consent from those being filmed, and provides strict penalties for doing so without obtaining prior consent.

However, these protective provisions may be easily circumvented by the police, by making use of the broad exemption provisions in favour of Government agencies, as provided under the Bill. Further, if such recording is done under direction of any Court or Tribunal in India, then the Bill provides an exception from the need to obtain consent in that case.

*

Vaneesha Jain is an Associate Partner at Saikrishna & Associates, and works on Policy matters, in addition to advising clients in the fields of intellectual property, information technology and data privacy. She is currently based out of Bangalore. The views expressed in this article are solely the author's.

Edited by Aditi Agrawal

Personal Data Protection Bill, 2019: Will it rid us of pesky and creepy ads?

As the Joint Parliamentary Committee considers the Personal Data Protection Bill, 2019, MediaNama will publish a series of articles from legal experts focussing on the key aspects of the Bill and how they will affect users and companies. This is the seventh article in the series. Read our extensive coverage of the Bill here.

By Divij Joshi

Ever get the strange feeling you're being watched online? When a 'real-life' conversation about food cravings results in an eerily similar restaurant ad on a totally unrelated website? Welcome to the 'uncanny valley' of targeted advertising.

Targeted advertising is the goldfield of the contemporary internet — the revenue backbone of social media, search engines, e-commerce and all of the ubiquitous 'free stuff' that fights for our online attention. The practices behind this business model have some troubling implications for online privacy. An instructive post by Sajjan Poovayya and Priyadarshi Banerjee outlined how the data collection of social media intermediaries may be affected by India's forthcoming personal data protection law. The advertising ecosystem is inseparable from the online economy and social media in particular, and deserves some further interrogation. In this post, I want to unpack the practical application of the PDP Bill's provisions to an increasingly popular advertising business model known as Real Time Bidding.

What is Real Time Bidding?

Online advertisements are increasingly placed using programmatic or automated systems, which apply sophisticated algorithmic rules to place advertisements targeted specifically towards the individuals browsing particular online publishers. In order to 'improve' the targeting of a particular user (to sell more relevant or purchasable ads from an ad company's perspective), companies require personal information about the individual visitor. This information is collected via a number of online tracking mechanisms using a number of tools — including cookies, device or browser fingerprinting or the use of tracking pixels, which track browsing activity across the web. These may be tools implemented by the publisher, or by third-parties who use the publisher's system to place cookies.

In simplified terms, Real Time Bidding or RTB is the system by which this information is collected, analysed and used for the purpose of serving ads. The information collected by publishers and by cookies is first sent to 'supply side platforms' (SSPs), who operate alongside 'ad exchanges' to connect publishers (or users, rather) with advertisers. The information is incorporated by SSPs into a 'bid request', which is broadcast to advertisers who compete to land 'impressions'.

sions' to specific individuals, through a near-instantaneous auction mechanism where every individual user and their information is 'sold' to these advertisers (or their agents). For an advertiser looking for an ideal 'target', the more information they have about a user, the greater the price they are willing to pay to an ad exchange for placing an ad, or an 'impression' on that user. The supply side of the advertising ecosystem therefore has an incentive to collect as much information about individuals and ultimately profile them for the purposes of selling to advertisers. These processes are largely governed by industry standards such as Google's Authorized Buyer's Framework or the IAB's OpenRTB system. (This diagram gives a simplified version of different actors within an RTB framework.)

At each level of operation of the advertising ecosystem — from the time someone loads a website to the time that they receive a targeted advertisement, multiple players are interacting and engaging in complex processes for shunting and processing personal information across the internet. Sensitive information (the most valuable to advertisers) is tracked and shared across multiple actors and databases, profiles are created about individuals using algorithmic logics, usually without the informed and continuing consent of the data principles. This is antithetical to accepted principles of data protection, including the right to informational self-determination as a constituent element of the fundamental right to privacy under the Constitution of India.

The burning question is — how does the recently introduced Personal Data Protection Bill map onto this complex ecosystem? Does it protect online consumers from rampant data extractivism and profiling?

The Personal Data Protection Bill — Reform or Relapse?

The PDP Bill attempts to place individual choice and autonomy at the heart of the data protection regime. The foremost is the requirement of informed consent before personal data can be collected or processed, under Sections 7 and 11. Further, the Bill requires personal data to be collected and used only for specific and clearly defined purposes, and only to the extent necessary for such purposes.

The PDP Bill also includes certain additional protections against 'profiling', which is defined as data processing that analyses or predicts user behavior and attributes. Data pertaining to children (Section 16), as well as sensitive personal data (Section 15), may be prohibited or require additional safeguards against profiling. However, these safeguards will not kick in until the Data Protection Authority under the Bill notifies and makes such protections applicable.

The definition of Personal Data under the PDP Bill includes all information by which a natural person (an individual) is directly or indirectly identifiable, including inferences made about such individuals. Any information which allows an individual to be specifically targeted, whether online or offline, will fall within this definition. Generally, the information collected by the RTB system includes

identity information such as an IP Address, or the ‘fingerprint’ from a device or browser — which are squarely relatable to individuals and fall under the category of personal data. In addition, information such as location data, timezone or other information can similarly be combined to identify an individual, and such combinations would also fall under the scope of the PDP Bill. These categories of data are often also used to make additional inferences about an individual, for example, correlating location data to financial data. In addition, certain RTB protocols also collect information relating to political affiliations, health status, sex or sexual orientation. This information falls under a special category of data known as ‘sensitive personal data’, and for which there exist additional protections under the Bill (although these additional protections will need to be notified by the Data Protection Authority).

Most of the information collected under contemporary RTB systems can therefore safely be assumed to fall under the PDP Bill’s scope.

Who is responsible for maintaining the protection of personal data?

The PDP creates two categories of data processors — the data ‘fiduciary’, which is defined as the entity which controls the purpose for which the data was collected and processed; and the data processor, who may process data on behalf of the data fiduciary. **The primary responsibility of data protection vis-à-vis a data subject is on the data fiduciary.**

Determining the roles and responsibilities of each entity involved is perhaps the biggest challenge for operators as well as consumers in the ad-tech scenario. The large number of entities determining the means and the purpose of collecting and processing data means that there will be multiple entities with the responsibilities of a data fiduciary for the same data subject. In addition, there are hundreds of other entities to whom information is ‘broadcasted’ in the ‘bid request’ for the purpose of returning an automated bid. **While Section 31 of the PDP Bill requires that every data processor working on behalf of the data fiduciary must enter into a contract for the same, with the hundreds of entities involved, this becomes effectively impossible.** Further, certain publishers or entities like data brokers or social media companies may also qualify as ‘significant data fiduciaries’ under Section 26-30, have additional obligation in relation to their data collection and processing.

For an ordinary web user, there are severe challenges to their ability to control personal data. The current mechanisms for consent are entirely unmanageable and impossible to comprehend, let alone control. Although mechanisms like the ‘consent manager’ sought to be introduced under Section 23 may go some way into rectifying this problem, it is no easy task to reign in the complex data flows permitted by the RTB system. For example, companies are attempting to comply with the requirement of ‘notice and consent’ by providing ‘clickwrap’ consent notices which mean that users are expected to read through hundreds of privacy

policies before following through on a publisher's webpage. Additionally, the algorithmic logic and specific data used to profile and classify individuals (ranging from inferences about financial status, to gender and sexuality and caste) are unknown to users, even though it may affect the nature of advertisements they receive. However, the dependence of internet commerce on programmatic ads means that users are left with a Hobson's choice — to 'consent', or to be locked out of the web.

Conclusion

Barring some exceptions, the provisions of the PDP Bill appear to severely curtain the collection, processing and sharing of personal data within the online advertisement space and under RTB. However, experience from Europe indicates that the very business model of online advertising may be fundamentally incompatible with requirements of informed notice and consent under data protection laws. As a recent study by Karolina Iwańska and Harriet Kingaby indicates, this model of online advertising may be fundamentally broken beyond repair.

RTB (and other forms of programmatic advertisements) may be antithetical to data protection inasmuch as it is driven by the requirement that personal information be collected and broadcast across hundreds or thousands of entities with no technical or governance mechanism to keep such data sharing in check. Such practices and their potential non-compliance with the GDPR are already coming under the scrutiny of various executive and judicial authorities, including the UK's ICO and Norway's consumer protection agency, which have categorically determined that RTB violates European and national data protection law, and urged for courts and governments to enforce law by intervening in the RTB system.

Any reform of programmatic advertising and its harms to users, under the PDP Bill, may ultimately be question of the DPA's capacity and willingness to enforce the principles of purpose limitation, informed notice and consent, as well as its ability to make progressive regulations to protect against individual profiling. The broader question however, is whether an internet economy rooted in capturing and monetising every iota of our attention can ever be compatible with our established and emerging norms of online privacy, and how the ad-tech system can embody principles of data minimisation and privacy by design in their technical and commercial choices.

*

Divij Joshi is a lawyer and a legal researcher, currently researching artificial intelligence and automated systems, as a Mozilla Tech Policy Fellow. He can be reached on Twitter at @divijualsuspect.

Edited by Aditi Agrawal

Does the Personal Data Protection Bill, 2019, protect citizens' privacy from government surveillance?

As the Joint Parliamentary Committee considers the Personal Data Protection Bill, 2019, MediaNama will publish a series of articles from legal experts focussing on the key aspects of the Bill and how they will affect users and companies. This is the eighth article in the series. Read our extensive coverage of the Bill here.

By Pallavi Bedi

*

A government agency buys surveillance software from a foreign company. It then plants the software in the devices of Indian citizens. The device company, that also operates a number of apps, discovers the software and sues the foreign company. Can the DPA investigate the government agency?

The suit filed by WhatsApp in a Northern California court against the Israeli cyber-intelligence company, NSO Group Technologies, laid bare the nefarious intrusions of the global surveillance industry into the protection of civil liberties and the trajectory of geo-politics narratives. WhatsApp alleged that the NSO group had deployed the Pegasus spyware to conduct targeted surveillance on the cellphones of over 1,400 lawyers and human rights activists all over the world, including from India.

Given NSO's statements claiming that they only sell services to state governments, there was widespread suggestion that the Indian government had deployed Pegasus to target dissenters against the ruling government. On November 29, 2019, the IT Minister, Ravi Shankar Prasad failed to categorically deny that the Indian government had used Pegasus to spy on its own citizens, instead merely claiming that "standard operating procedures have been followed."

The government derives its power and authorisation to conduct surveillance from Section 69 of the Information Technology Act (IT Act), read with the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information Rules), 2009 (IT Rules). The rules lay down the procedure to be followed by the government agencies to undertake electronic surveillance. It is pertinent to note that the IT Act — under Section 43 and Section 66 — penalises any unauthorised access to computer systems, and the government has not been granted any exception.

On November 19, 2019 in response to a specific question on whether the government was tapping WhatsApp's calls and messages, the Minister of State in the Ministry of Home Affairs, G. Kishan Reddy, referred to the procedure prescribed under Section 69 of the IT Act and under Rule 5 of the Indian Telegraph Act and stated that only 10 agencies authorised by the Ministry of Home Affairs

were permitted to undertake any interception or monitoring.

The global surveillance industry is a dangerous, strategic conglomeration of states adopting an increasingly authoritarian approach to the use of technology, and the private sector are willing allies in a bid to rake up profits at the expense of civil liberties. The possibility of entrenched networked surveillance today makes this scenario a critical one for understanding the efficacy of the proposed Personal Data Protection Bill. Can its provisions and the authorities empowered by it genuinely preserve privacy in India today?

How will the Central Government, WhatsApp and NSO be classified under the Bill?

The Central Government and WhatsApp can be classified as data fiduciaries under the Bill as they determine the means and purposes of processing of personal data. The users of WhatsApp in India will be regarded as ‘data principal’.

The jurisdiction of the Bill is country-agnostic as long as the data fiduciary ‘offers services to data principles within the territory of India’ and therefore, WhatsApp will come within the ambit of the Bill and it will be required to comply with the obligations specified in the Bill.

On the other hand, the NSO may not be regarded as a data fiduciary as its role appears to be limited to providing the surveillance tools to the State — it does not determine the purpose and means for which such surveillance tools will be used — that is left to the State.

Can the DPA investigate a government agency and WhatsApp?

The Bill establishes a Data Protection Authority (DPA) to ‘protect the interests of the data principal, prevent any misuse of personal data and ensure compliance with the provisions of the Bill’. Under the Bill, the DPA has the authority over the processing of personal data by private data fiduciaries as well as the State.

An important obligation of the data fiduciary under the Bill is to maintain transparency while processing personal data and as part of this obligation, Section 23 (1)(e) requires the data fiduciary to inform the data principal about the right to file a complaint against it before the DPA. Further, section 53 (1) provides that the DPA can either *suo-motu* or on a complaint received by it inquire into the activities of any data fiduciary, if the activities are being conducted in a manner which are detrimental to the interests of the data principal.

Once the complaint is received, the DPA is required to issue a written order appointing an Inquiry officer responsible for conducting an inquiry and submitting a report to it. Upon receipt of the report, the Bill specifies the measures that the DPA can undertake — these range from reprimanding the data fiduciary to temporarily suspending the activities of the data fiduciary which are in

contravention of the Bill.

How will this work in practice?

In theory, the Bill provides the framework for any data principal to file a complaint before the DPA against the actions of a government agency and WhatsApp and for the DPA to initiate an inquiry. However, the extensive exemptions powers given to the Central Government under the Bill belies this expectation.

The 2018 Bill sanctioned processing of personal data by intelligence agencies and law enforcement officials and exempted such authorities from certain provisions of the Bill. However, such sanction to either intelligence officials or law enforcement agencies was subject to it being (a) authorised by law; (b) in accordance with the procedure laid down by the law; and (c) necessary and proportionate. This four-step process embeds the principle laid down by the Supreme Court in Right to Privacy judgement (*Puttaswamy v. Union of India* [2017]). This was regarded as a first step towards determining the surveillance powers of the State and the expectation was that the government would further strengthen the provision to streamline and regulate the surveillance apparatus.

However, the present Bill has the opposite effect — instead of regulating surveillance, it has augmented the government's surveillance power. Section 35 now provides that the Central Government can exempt any agency from **all or any provision** of the Bill if it is necessary or expedient to do so in the interests of (a) sovereignty and integrity of India, national security, friendly relations with foreign states, and public order or (b) for preventing incitement to the commission of a cognizable offence relating to (a). The four-stage test proposed in the Puttaswamy judgement has been done away with. Further, the procedure to be employed and the oversight mechanism to be followed by the exempted government agency (exempted by the Central Government under this provision) will be prescribed in the future

By virtue of Section 35, the government can exempt the surveillance and law enforcement agencies from the jurisdiction of the DPA. In addition, the government can also exempt such agencies from all the transparency and accountability requirements specified in the Bill. Therefore, the affected data principal may never be notified about the processing of her personal data by law enforcement agencies and/or surveillance agencies, and therefore will not be able to file a complaint before the DPA.

An essential obligation of the data fiduciary under the Bill is to implement necessary security safeguard features considering the nature and purpose of processing of personal data. WhatsApp could argue that it has employed end-to-end encryption for all messages and calls by default and that it has sought a permanent injunction banning NSO from using its service, thereby complying with this requirement.

Therefore, despite having jurisdiction, in practice, the DPA will be unable to

adequately protect the rights of the data principal. This means that alternate means of preventing the development, testing, sale and transfer of surveillance technology will need to be devised at the national and global levels.

*

Pallavi Bedi is a senior policy officer at the Centre for Internet & Society. This article was written with inputs from Arindrajit Basu.

Edited by Trisha Jalan

How will India's Personal Data Protection Bill, 2019 impact schools?

As the Joint Parliamentary Committee considers the Personal Data Protection Bill, 2019, MediaNama will publish a series of articles from legal experts focussing on the key aspects of the Bill and how they will affect users and companies. This is the ninth article in the series. Read our extensive coverage of the Bill here.

By Rahul Narayan

As thousands of anxious parents are busy filling forms for school admissions, and all the schools are engaged in the mammoth yet intricate task of sifting through thousands of forms to find “suitable candidates for admission”, it is a truth that needs to be universally acknowledged that the system works on the principle of “*give me your data and I will give you ... admission*”. Indeed, in the entire school journey from admission to graduation to alumni, schools collect data, store data, process data and generate data.

What kind of data do schools collect?

At admission, schools typically ask for names, ages, addresses, photographs, sex, religion, Aadhaar numbers#, birth certificates, details of siblings, parents' names, parents' qualifications, family income, telephone numbers, email addresses, etc. Once children are admitted, financial data such as bank account details, and health data such as blood group, allergies, weight, height, immunisations, regular medication (if any), dental check-ups, eye check-ups, etc. are added. Then there are progress reports, participation details, and disciplinary records of students which are generated by schools. Finally, there are contact details and achievements of alumni which are kept, in particular, for school fundraising, directories, even advertising, etc.

At every stage, schools collect and process personal data including sensitive personal data — financial data and health data —of their students *and* of their parents/guardians. **Consequently, the Personal Data Protection Bill (“the Bill”) has enormous ramifications for schools.**

How will the Bill classify schools?

There can be little doubt that schools are “data fiduciaries” for the purposes of the PDP Bill and as such, they are required to fulfil all obligations under Chapter II, that is, Sections 4 to 11, particularly those dealing with purpose limitation, the requirement of consent, etc., as well as the accountability and transparency measures specified in Chapter VI. Since schools inevitably process large volumes of personal data of children, they will also be regulated as guardian data fiduciaries for the purpose of Chapter IV of the PDP Bill and the regulations made under them. Considering the volume and sensitivity of

personal data processed, the Data Protection Authority (DPA) may also seek to regulate schools as Significant Data Fiduciaries under Section 26 of the Bill. Government run schools may also be regulated differently if they are classified as a “service provided by a government” under Section 12(a)(i) of the Bill.

Schools, like other data fiduciaries, will thus be required to prepare a “privacy by design” policy dealing with practices and systems to anticipate, identify and avoid harm to the students or former students, ensure technological processing is in accordance with certified standards, and to ensure that the processing has to be secure at all stages. They also have to comply with the requirements for transparency in processing, and for data security. If schools are classified as Significant Data Fiduciaries, they will be required to appoint Data Protection Officers, carry out data protection impact assessments in case they process data through new technology, and maintain records and carry out annual data audits.

What does all this entail in terms of how schools operate? Quite a lot actually. Consider the following questions as a kind of sample of what needs to be tackled:

Will schools have to change the way their admission forms are drafted and processed?

Simply put, yes they will — both in terms of content and in terms of processing.

Content of admission form:

1. **Purpose limitation:** In terms of data required, forms will have to be limited to data that is connected or incidental to the “specific, clear and lawful purpose” of ensuring admission to an educational institution. The notification dated January 6, 2016 issued by the Department of Education already regulates what can be asked this to a large extent though this has been challenged before the Delhi High Court (W.P. (C) No. 448/2016) and awaits a final decision. It is pertinent to note that admission cannot be denied or made conditional on consent to processing of any personal data not necessary for admission.
2. **Taking consent:** The form will also have to explain in simple and easily comprehensible language(s) the nature and categories of personal data collected, the duration of time such data is stored, the identities of whomsoever such data may be shared with, details of the rights and remedies available to the persons whose data is collected, the procedure for grievance redressal, etc. The essential requirement is the free, informed, specific, and clear consent that may be withdrawn. **The burden of showing that the consent taken was informed consent rests upon the schools.**
3. **Separate consent for sensitive personal data:** Since some of the data collected will be sensitive personal data (such as health and financial data), the form will be explicitly required to inform the parents/guardians in clear terms the purpose of or operation in processing that is likely to

cause significant harm. The parents will also have to be given a choice of separately consenting to different categories of sensitive personal data.

- Government schools provide a service from the state and thus may be exempt from some of the rigors of obtaining consent as distinct from private schools. However, the boundaries of such exemption are unclear under section 12(a)(i) of the Bill.

Processing of admission data:

1. **The school is responsible for compliance with the requirements of the PDP Bill for any processing that is carried out on its behalf.** This would entail an overhaul of the mechanisms currently used to process applications. If data processors are hired, they will need to be monitored to ensure compliance. Such data processors may only be appointed vide a contract and are bound by the instructions of the Data Fiduciary and must treat data as confidential as per Section 31 of the Bill.
2. Schools would also need **a policy to destroy or delete such data collected at the end of the admission process** and set up a time frame in this regard erring on the side of lesser rather than greater time of retention. Applications that do not lead to a successful admission ought not to be kept beyond a reasonable time frame following the draw of lots. For successful candidates, such data as is required by law must be maintained. For retention of other data for any purpose, explicit consent of the parents/guardians will be necessary.
3. Policies framed for data processing, data retention and data destruction will have to take into account that **there is a general obligation that personal data of the child is to be processed in a manner that protects the rights of the child and which must be in her best interest.** Schools, as likely guardian data fiduciaries, shall be barred from profiling, tracking, or behaviourally monitoring of children or undertaking any processing that can cause significant harm to the child.

Can schools share sensitive personal details of children such as health data?

Usually they cannot —especially not without the consent of the parents or guardians in case of minors. As a guardian data fiduciary, schools have an additional duty to avoid processing of personal data that can cause significant harm to the child.

However, an explicit exception is made to respond to a medical emergency involving a severe threat to the death of the individual or to provide treatment or services during an epidemic or threat to public health, as per Section 12(e) of the Bill.

How must schools deal with data they generate — such as performance records, report cards, etc?

School report cards, performance reports, and suspension letters all fall in the category of personal data. As such, they cannot be shared without prior explicit consent except for specific and limited grounds contained in Sections 12 and 13 of the PDP Bill. Sharing of data with the education boards, for example, will probably be mandated. Sharing data in case of transferring students would usually happen with the consent of the parents of the transferring children. However, there are aspects of this that are tricky. What happens if the parents want deleted reference to disciplinary inquiries or issues like bed wetting from the records?

Under section 9 of the Bill, students, as data principals, have the right to ask for erasure of personal data that is no longer necessary for the purpose for which it was created. This would cover old disciplinary records or performance certificates. Schools have the right to refuse to do this if they have adequate justification which they explain to the Student. If the student is dissatisfied with the justification, she has the right to insist that the data contains a caveat that it is disputed by the student.

Students may also argue that such data processing may cause significant harm or amounts to profiling, tracking or behavioural monitoring, which are expressly barred for guardian data fiduciaries such as Schools under Section 16(5) of the Bill at the risk of penalties under Section 57(2)(b). It is not a stretch to see that performance records, report cards and the like could be construed to be data that amounts to profiling, tracking or behaviourally monitoring of children, particularly when such data is compiled on an annual basis.

Until Regulations under section 16(6) are framed, it would be difficult to see how schools are to deal with this. **This broad ban under Section 16(5) makes sense for guardian data fiduciaries that deal with e-commerce or gaming, but is overbroad and even counter-productive for educational institutions such as schools that ought to track, profile, or monitor at least some of what children are up to with a view to enhancing the educational experience.** Should schools be able to monitor what websites children go to when they use school computers? Should teachers be able to profile kids being considered for scholarships or those that may be at risk? Under Section 16(5) of the Bill, they cannot.

Regulations by the Data Protection Authority under Section 16(6) may modify their applicability for data fiduciaries that offer “counselling or child protection services to the child” though schools may need a broader carve out for traditional pedagogical functions. Rather than a broad ban and a narrow exception, the contours of which will be decided by regulation, it may be more prudent to exempt schools and educational institutions with respect to their activities related to learning or welfare while banning profiling or tracking that is linked to say religion or race or sexuality.

Students and former students have, in addition to other rights, the right to be forgotten to prevent disclosure of personal data under Section 20 of the Bill. This right can be exercised subject to the order of an adjudicating officer who must balance this right with the right to free speech and expression and keeping in mind, for example, the role of the former student in public life.

Conclusion

Data protection and its relationship with the ancient right of privacy have been debated and argued in the developed world since at least the 1970s. Principles have evolved and developed organically, frequently from bottom up. In India, however, this dialogue only really began after the Supreme Court re-affirmed the right to privacy in *Puttaswamy I* and dealt with the Aadhaar Scheme in *Puttaswamy II*. The PDP Bill, when enacted, will be the first significant data protection act in India. We don't have much past practice or experience to guide us how to interpret the broad principles the Bill identifies. What final principles end up being adopted will depend on many factors such as the composition of the data protection authority, the enforcement of the rights conferred by the bill and most of all by industry practice and regulations.

For schools, many ticklish practical questions relating to data protection will need to be ironed out, in particular because of the quality and quantity of data they collect of children. Would data of children have to be anonymised to even higher specifications than data of adults to prevent any possible use that could lead to significant harm in case of government request for data? To what extent are schools permitted to share student data with colleges when the latter request the former for verification? What happens when verification requires sensitive personal data to be transferred out of the country? How will the restrictions imposed on checking student behavioural patterns be interpreted by the data protection authority and by the courts? Can school teachers use examination results and other records to offer tuition to students? Do alumni directories violate the principles of data protection? Can schools use parents' financial information to solicit funds?

Schools will need to be schooled.

This is specifically barred under the *Puttawamy II* judgment.

*

Rahul Narayan is an Advocate-on-Record in the Supreme Court of India. He has appeared in matters involving the right to privacy, access to internet, intermediary liability and digital rights. He also advises companies and institutions on issues relating to compliance with technology law, and cyber frauds. He can be reached at Rahulnarayan@lawfirst.in.

Edited by Aditi Agrawal

Personal Data Protection Bill, 2019: Considering impact on the healthcare sector

As the Joint Parliamentary Committee considers the Personal Data Protection Bill, 2019, MediaNama will publish a series of articles from legal experts focussing on the key aspects of the Bill and how they will affect users and companies. This is the tenth article in the series. Read our extensive coverage of the Bill here.

By Abhishek Malhotra and Bagmisikha Puhan

In the ambivalent situation that the healthcare sector finds itself in the middle of, the proposed data privacy and protection legislation lends direction to the stakeholders of this sector, that include healthcare providers, patients, caregivers, and other interested parties. The proposed legislation is timely, in that, the overlapping, co-dependent sectors, currently plagued with lack of uniformity in technical and organisational standards, will get the requisite impetus to align their approach and achieve efficiency in delivery of the services.

Section 2 (21) defines health data as *data related to the state of physical or mental health of the data principal and includes records regarding the past, present or future state of the health of such data principal, data collected in the course of registration for, or provision of health services, data associating the data principal to the provision of specific health services.* In this present form, the proposed legislation encompasses the entire life cycle of a person's health information. The present healthcare set-up has evolved into a stage where the patients now prefer continuity of care, and their expectations regarding the preservation of health data/records ranges from womb to tomb.

Lack of data processing standards across the sector

In India, the healthcare set-ups are acutely heterogenous and do not interact with one another, which takes away from the end users the control over their own data, and the flow/management of their records. This extends beyond the care delivery set-ups, and also extends to the networks on which the product delivery platforms operate on (both brick and mortar, and online models).

While the proposed legislation deals with the creation, handling and management of personal and sensitive personal data, the Bill does not designate the individual (in this case, the patient) as the owner of the data pertaining to them. While the Bill's definition of data accounts for *representation, of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means,* the manner in which a General Practitioner (GP) in the country maintains records of his/her interactions with the patients are not in-line with the systems of a private hospital. Further, the proposed legislation assumes that the systems

within the ecosystem are capable of interacting with one another. That is not the way the healthcare sector operates in the country as healthcare providers, GPs and online platforms all use different technical standards. To facilitate seamless interactions across the sector, specific technical standards will have to be adopted/introduced.

Would a general practitioner and a hospital be equally liable?

The distinction between the compliance requirements of a GP and a larger hospital set-up would be in terms of the volumes of personal/sensitive personal data that is created and processed by the concerned entity. The concept of significant data fiduciaries (SDFs) would be attracted as per the levels of processing and would put the SDF in a position which requires stricter levels of compliance. Requirements like ensuring audits are conducted, and audit trails are maintained; along with the onerous, yet necessary, requirement of conducting a data protection impact assessment will be imposed on such hospitals. While this distinction will impact the level of compliance required of both the entities, the GPs will not be absolved of the requirements pertaining to confidentiality, integrity and accessibility of the personal/sensitive personal data sets. The GPs will have to ensure that they do not run afoul of the rights of the data principals, such as the right to access and to port the data to another healthcare service provider. When data is ported from an individual practitioner to a larger, organised set-up, homogeneity standards may come into play. The GPs would also need to comply with the requirements of provisioning of available data in a format/manner which is conducive for transfer from one unit to another in the best interests and at the instance of the data principal.

Is transferring patient records the same as porting data under right to portability?

Transfer of electronic health records, and electronic medical records qualifies as an extension of the right to portability whereby the data which may be sought to be ported must be raw data. For instance, assessment of health data will be inferred or derived data and may not fall within the scope of data portability, as with GDPR. Subject to further guidance, it will have to be evaluated whether data not provided by the data principal will be within the scope of this new right, and the extent as such.

The GP is expected to comply with the requirements prescribed under the proposed legislation, and must ensure that s/he relays and explains to new and existing patients the initiation of an interaction, continuation of treatment, and the expected consequences of such relationship created between the two individuals. Deriving from the expected National Digital Health Blueprint, the system is moving towards a synchronous and interactive framework, where the flow of information between the stakeholders is not restricted and is expected to be secure at all times. The National Digital Health Blueprint will have to

comply with the Bill once it becomes a law.

What happens in an emergency situation?

Going by how the sector operates in its current form, should a patient require urgent attention, it is upon the patient or his/her caregiver to bring in the old records to the hospital/clinic (formal set-up) for follow-up, validation, and further treatment. The Bill does not take away the requirements prescribed under the existing laws governing the healthcare sector. The Indian Medical Council (Professional Conduct, Etiquette, Ethics) Regulations, 2002, prescribes for the healthcare providers to maintain medical records in a desirable manner, and also urges for the computerisation of such medical records for quick retrieval. The proposed legislation is working in consonance with the existing approach and expects of all the stakeholders a similar level of compliance.

What happens when you order medicines or book diagnostics online?

For a user, the choice of consulting a physician from the options provided on the internet is based on the cost of the consult, availability of the physician and the location of the healthcare provider/ institution. All of these parameters are also accessible freely.

Most of these websites step beyond their designated roles of being facilitators and conduits to the more challenging role of an intermediary whereby they allow a user to book diagnostic tests, and to order medicines online. In doing so, the website needs to evaluate the prescription, which may be uploaded by the user directly, or may have been generated by the physician or consult made available by the website itself. In either scenario, the website is privy to the contents of such laboratory test results, diagnostic reports, prescriptions, and other captured information.

All of this information qualifies as sensitive personal data owing to the nature of the identifiers. **The liabilities of such a website will be similar to that of a data fiduciary which creates, consumes and processes personal/sensitive personal data in large volumes, and in all likelihood will qualify as an SDF.** The websites will be required to adhere to a certain level of technical and organisational standard which will be slightly higher than the standards prescribed for a GP. This will be owing to the number of processes and people who will be involved in processing the data pertaining to the large numbers of the end users. Further, the proposed legislation may lend further guidance in terms of the technical standards that the larger institutions will be subjected to, in contrast to what may be prescribed for a GP. **It is essential to note the difference that would exist between the ones employed by the GP and the ones deployed by the website, or a larger institution.** It is these nuances which will also impact the extent and the scope of liabilities that the entities will be subjected to, respectively.

Conclusion

Seemingly, there will be no additional riders under the proposed legislation, however, we may expect a guidance document or a policy document concerning the sector to come up for further understanding and effective implementation of the processes. However, in the meanwhile, the basic compliance requirements of proper and valid notices, explicit and specific consent, will have to be maintained and cannot be compromised by an individual practitioner, or a website.

The proposed legislation does not differentiate between the pedigree and the magnanimity of the data fiduciary on the basic compliance requirements. However, further compliance requirements are proposed in a manner which is proportional to the nature and scale of processing of personal and sensitive personal data of the individuals. **The liability that any entity will be subjected to under the proposed law will depend on the extent of the data being processed, the extent of dereliction and the effective controls which supposedly were in place for efficiency.**

*

***Abhishek Malhotra** is the Managing Partner of TMT Law Practice. He has over 20 years of experience in dispute resolution and corporate advisory and actively participates in the development of policy and jurisprudence in the TMT sector, focusing on emerging technologies and the healthcare sector.*

***Bagmisikha Puhan** is a Senior Associate at TMT Law Practice who specialises in technology law and advises clients in the ITeS, media, healthcare and pharmaceuticals, space sectors. A member of the Telemedicine Society of India, she also conducts capacity-building and training programmes. She has worked extensively in matters pertaining to the data privacy and data protection laws of several jurisdictions.*

Edited by Aditi Agrawal

****Update (11:37 am): The headline was updated.*

Personal Data Protection Bill, 2019: Considering its impact on housing societies

As the Joint Parliamentary Committee considers the Personal Data Protection Bill, 2019, MediaNama will publish a series of articles from legal experts focussing on the key aspects of the Bill and how they will affect users and companies. This is the eleventh article in the series. Read our extensive coverage of the Bill here.

By Jyotsna Jayaram

Administrative staff (including security personnel) engaged by housing societies and apartment associations often transform into persons of authority when they are tasked with the responsibility of screening, and recording details of, guests or residents before they enter the premises. More often than not, in an almost police like manner, they ask an entrant to provide several details about themselves such as their name, address, mobile number, vehicle number and, sometimes, even a proof of identity. While conventionally all of this information was jotted down in musty hardbound paper registers, several housing society/community management apps have recently begun to replace the stacks of registers and ball-pens that would be used by these personnel to document entrants. With the introduction of the proposed Personal Data Protection Bill, 2019 (the Bill), a seemingly routine activity could suddenly find itself subject to a number of compliances that these housing societies and apartment associations possibly had not anticipated.

Do housing societies collect personal data?

Housing societies typically collect the name, address, phone number, and vehicle number of visitors. At times, they also take a photograph at the time of entry. Therefore, the information collected by housing societies and associations has always been within the realm of ‘personal information’ even under India’s existing data protection framework under the Information Technology Act, 2000. Personal information has traditionally been defined to mean “*any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person*”. The Bill, widens this definition to include data that has regard to any characteristic, trait, attribute or any other feature of identity of a person, whether online or offline. In this context, it bears mentioning that the Bill applies to processing of personal data by humans *and* by automated means, though it does carve out some exemptions for manual processing. However, the requirement to obtain consent of the entrants or residents, or to implement robust security safeguards for the collection and processing of such information are new asks and something that the processes adopted by housing societies possibly do not contemplate.

Are housing societies data fiduciaries?

Section 2(13) of the Bill defines data fiduciaries to mean “*any person, including the State, a company, a juristic entity or any individual who alone or in conjunction with others determines the purposes and means of processing of personal data*”. In a marked departure from the existing regime, the Bill also applies to individuals who process personal data of others. The Bill defines ‘person’ to include “*an association of persons or a body of individuals, whether incorporated or not*”.

Housing societies or apartment associations are typically registered societies and therefore have a separate juristic personality. Housing societies collect personal information of residents as well as of other entrants for several purposes, including security and safety of their residents. **Therefore, they would be considered data fiduciaries under the Bill.** Consequently, all the obligations that apply to data fiduciaries under the Bill, such as the requirement to provide notice, obtain consent, and implement necessary security safeguards, would apply to these societies.

The Bill also regulates a class of data fiduciaries known as significant data fiduciaries that may be classified as such by the Data Protection Authority based on factors such as the volume of data processed and the sensitivity of the data that is processed. In the absence of any guidance on this classification, a literal reading of these factors may suggest that housing societies, particularly those dealing with large residential complexes, may fall within this classification. **However, in my opinion, a housing society that primarily processes data for internal management and safety purposes and not commercial purposes ought not to be classified as an SDF, particularly because it is not data driven business and the purposes of processing are usually limited.**

While it is feasible for most corporate entities that deal with data as a part of their business to understand and comply with the requirements under the Bill, it remains to be seen how housing societies that comprise mostly of residents themselves will employ the necessary technological measures to comply with all the requirements of the Bill. This is particularly relevant as the types of individuals whose data housing societies normally collect is very diverse and could include children, family of the residents, domestic help, delivery agents, etc.

Putting consent into effect

One of the foremost requirements under the Bill is to provide notice to the data principal which, among other things, must specify the purposes for which personal data is to be processed, the nature and categories of personal data being collected, and the basis for processing. This notice must be “*clear, concise and easily comprehensible to a reasonable person and in multiple languages where necessary and practicable*”. Given the diverse categories of data principals and

the different purposes for which their data will be collected, it is likely that housing societies would need to have several customised notices which may be used based on the data principal. For instance, the notice provided to a resident would be entirely different from a notice provided to an Amazon delivery agent whose data is collected before he delivers a package to a resident.

Could housing societies be exempted from the provisions of the Bill?

While the Bill does provide for certain non-consensual grounds of processing (such as actions by the state, for the purposes of employment or for reasonable purposes as specified by the Data Protection Authority), none of these grounds in their present form would be available to the processing of personal data by housing societies. Having said that, Section 36 of the Bill exempts the applicability of certain chapters of the Bill where personal data is processed *inter alia* in the interests of prevention and detection of any offence. Unlike other exemptions that apply specifically to the State, this section does not seem to exclude the processing of personal data for this purpose by non-State functions, such as for instance the use of CCTV cameras in a commercial complex. It is therefore possible to argue that the collection of personal data by housing societies in the interest of ensuring safety of their residents should fall within the purview of this exemption, and consequently several provisions of the Bill ought not to apply. **However, given that the purposes for which a housing society collects personal information of residents and entrants vary and are not only in the interest of security, this argument can be made only in respect of the information that is collected by the society solely for safety reasons and such a distinction may not, in fact, be feasible.**

Would a housing society be considered a ‘small entity’?

Section 39 of the Bill provides for certain exemptions for the manual processing of personal data by small entities. The Bill does not specifically define this term and yet again leaves this determination to the Data Protection Authority who will classify a data fiduciary as a ‘small entity’ based on factors such as its turnover, the purpose of collection of personal data for disclosure to other persons, and the volume of the personal data processed by the data fiduciary.

Manual processing (including collection) of personal data by a data fiduciary that is classified as a small entity will be exempt from several provisions of the Bill, including the provisions that pertain to notice, data quality, data retention, privacy by design and security safeguards. While this classification would certainly benefit non-digital businesses, in the absence of a specific definition or thresholds, it is unclear which entities would be classified as small entities. Therefore, at this point, there is no certainty whether housing societies that continue to collect and process data manually would qualify as small entities.

What happens when data is not processed manually?

Visitor and community management apps are now a common feature in most residential complexes and bring with them several additional features that appear to be quite beneficial to residents. For instance, a resident will know each time that their domestic help enters the gate and leaves the premises. Similarly, the resident will be prompted to approve the entry of a delivery agent on the app before they are permitted to enter the premises. As a part of these features, the app will create a profile of each entrant which at the very least has their name, photograph and mobile number along with a description of who they are – such as plumber, driver, delivery agent. Consequently, several additional categories of personal information may be collected as a result of using these apps.

As data fiduciaries, housing societies would continue to remain primarily responsible for the collection and processing of personal data even if they rely on visitor and community management apps. Therefore, in addition to implementing necessary measures and processes themselves, housing societies would need to ensure that the contracts with various community management app providers contain robust provisions on the processing of personal data to ensure that they are able to comply with their obligations under the Bill.

Visitor and community management apps such as MyGate would also need to take a look at their processing activities to clearly demarcate those activities that are being carried out on behalf of their client, that is, the housing society, and any processing that they may carry out to provide services to the residents directly, such as the information collected for creating resident accounts on the platform. This is relevant as these app providers could find themselves switching in and out of the role of a data processor and consequently attract varying obligations under the Bill. Having said that, this determination would differ from app to app, based on the manner in which the app functions and the services are provided.

Conclusion

Given all of the above, housing societies would need to take a close look at the manner of collection and use of personal data of its residents and entrants. A detailed analysis is necessary to determine the varying manner in which each requirement would need to be implemented keeping in mind the different categories of data principals whose data the housing societies would process. For instance, in relation to residents, housing societies are likely to process sensitive personal data (such as financial data for facilitating maintenance payments) in addition to personal data and this would be subject to additional compliances.

Further, some of the requirements under the Bill are in some instances practically infeasible to comply with. For example, when a child enters a neighbouring gated community to play with her friends after school, how is the housing soci-

ety going to ensure that age verification is conducted and that parental consent is obtained before they collect her name and address at the time of entry? Similarly, how will the housing society comply with requirement to obtain informed consent from domestic helps who are from different states and are not well versed in English and does this mean that they would need to provide notices in several vernacular languages? Evidently, the Bill has a significant impact on every section of society regardless of how internal or contained the processing may be. Therefore, **housing societies that so far may have been far removed from data protection regulation are likely to find themselves to be as much of a key player in the proposed regime as a data intensive business.**

*

Jyotsna Jayaram is a Counsel at Trilegal Bangalore and is part of the TMT practice group. She has a breadth of transactional and regulatory experience spanning over nine years. Some of her core areas of expertise include data privacy and cyber security, content regulation, digital communications and telecom licensing. Recently, she has extensively been involved in the submissions made by several industry stakeholders on the Personal Data Protection Bill, 2019.

Edited by Aditi Agrawal

Are matrimonial websites divorced from user privacy?

As the Joint Parliamentary Committee considers the Personal Data Protection Bill, 2019, MediaNama will publish a series of articles from legal experts focussing on the key aspects of the Bill and how they will affect users and companies. This is the twelfth article in the series. Read our extensive coverage of the Bill here.

By Kriti Trehan

As I sat to pen down this piece, my phone buzzed thrice in rapid succession. Distracted, as we oft are wont to be with alerts on our devices, I hastened to read the messages I had received. They were from family friends, following up on leads for a matrimonial alliance for their sibling. No, this is not my job; I just happen to know folks who know folks who are trying to get them married. Yet curiously, I received a plethora of information on the prospective party, including age, religious affiliation, employment details and a picture.

So without asking for it, I now had with me some incredibly private information about this person (which, needless to say, I purged from my device immediately). I had also, in the process, been entrusted to help find a match for this person. This meant that I would need to use this pool of information and compare it with another person's, and handling different individuals' personal information was just not an endeavour I was going to take on lightly. It was at this point that the sheer gravity of the responsibility upon matrimonial websites' proverbial shoulders dawned upon me. And things are about to get significantly more onerous (with good reason) under the proposed Personal Data Protection Bill, 2019 (the Bill).

Will the Bill cover matrimonial websites?

When I visited the websites of three of India's most prominent online matrimonial platforms, I noticed the wealth of information sought from a potential user at the stage of registration. Most of these sites required potential users to share a wide range of data: name, gender, date of birth, contact information, religion and mother tongue. Once registered, even more personal data is required to build the person's profile. For two of the three websites, employment and health information are mandatory requirements. Under the presently applicable Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules), all these categories of information qualify as personal information, with only gender and health crossing the threshold to "sensitive personal information".

However, the PDP Bill extends the definition of sensitive personal data to include religious affiliation, caste or tribe, and an expanded notion of financial

information. Under the Bill, personal data may be processed subject to *valid consent*, which means consent that is free, informed, specific, clear and capable of being withdrawn. In addition, processing *sensitive* personal data requires *explicit consent*, which means consent obtained must (i) inform the data subject about the purpose processing which may cause significant harm, (ii) be direct and not inferred, and (iii) be separate for different purposes and categories of sensitive personal data. Sensitive personal data can be processed without consent for state function, when required by law, to comply with judicial diktat, in cases of medical emergencies, and for ensuring safety and assistance in case of disasters or breakdown of public order.

Therefore, typically, to process some of the aforementioned categories of information, most of which are sensitive personal data, matrimonial websites will need valid and explicit consent. A quick check of privacy policies of these matrimonial websites disturbingly revealed that:

- Two of the three platforms, in their privacy policies, do not expressly state that the users' information is published or shared with other users on their service. While one may argue that this would be an obvious use case for information shared with a matrimonial website and therefore consent may be inferred, under the Bill, such a policy would fail to meet the compliance threshold.
- Two out of three websites don't have a consent mechanism built into the privacy policy to make the users' profile or snapshot thereof visible to non-registered users. In some platforms, the snapshot of the profile, which is visible to non-registered users, includes caste, religion and income related details. One platform shows user photos while two blur or remove them.
- Unlike data confidentiality which is typically protected by contractual arrangements, data privacy is protected by law. This means that data privacy has to be protected irrespective of whether or not it is contractually mandated. In this case, all three platforms contractually commit to data confidentiality but don't appear to fully carry it out.

Under the Bill, matrimonial websites will be well-served to reassess their privacy policies, make them clearer and more robust, and establish back-end processes in line with valid and explicit consent requirements.

Are matrimonial websites discriminatory?

News reports [editor's note: available here] from the United Kingdom earlier this month indicated that a leading matrimonial website had been hauled up for engaging in caste bias. The website has reportedly pushed back, of course, but this once again brings to the fore the question of whether or not matrimonial websites are inherently discriminatory as they allow for search parameters on religious and caste basis. My personal views on caste-based marriages aside, there are certain nuances that are relevant from a legal/policy perspective.

Let's begin with the obvious one — instances where users of matrimonial web-

sites opt to search for partners based on religion or caste, or where matrimonial websites establish microsites to cater to specific religions and castes appear to be in violation of fundamental rights under the Indian Constitution (on equality and rights against discrimination). However, there are two points to bear in mind in this context: first, fundamental rights under Part III of the Constitution of India are enforceable against the State, and not directly against private entities/persons; second, even if one were to proceed against the State for failing to uphold fundamental rights to equality and against discrimination, historically, by and large, courts have not been known to have meddled significantly with personal laws, especially since Part III itself enshrines the freedom to practice one's religion, freedom of speech and expression, and the right to life and personal liberty. Therefore, the likelihood of matrimonial websites being considered discriminatory in India seems low.

The other nuance, albeit semantic in nature, is no less important: where does this bias actually come from which then leads to what is arguably discrimination — in the algorithm of the website or does it emanate from the users and their preferences? Matrimonial websites create a platform where users have the ability to define their preferences, including on the basis of religion and caste. This is a double-edged sword. Websites, arguably, make these features available because of such a demand in society. The question is whether the platform is *creating* such discrimination, actively propagating it, or passively letting discrimination happen? I would think the website is a passive participant at best. Matrimonial websites create the ability for their users to choose, and so long as the platforms ensure the privacy and security of the data they handle, their operations are above board. Users can always choose *not* to give their preferences for religion and caste, or reveal it themselves. If, however, the bias emanates from the proverbial “ghosts in the machine” — the coding of the platform itself, it is a completely different ballgame. Where a matrimonial website, without seeking user preferences, shows only like-religion/like-caste matches, the risk (both actual and perceived) would likely increase exponentially.

With this background, an algorithm that makes caste/religion-based suggestions according to user preferences should not be found responsible for discriminatory harm. In this instance, I would find the platform upholding choice, which is the user's sacrosanct right under the consent, rights and transparency regime of the Bill. This right empowers the user to *not* share their data with the data fiduciary if it is not essential to the provision of services. However, at the same time, in line with the data minimisation principle, I would argue that asking for this caste-based information at the time of registration (irrespective of its usage to find matches) is excessive, and serves no tangible purpose for the user. At the very least, providing caste based information should be at the option of the user and not mandatory.

Does the Bill have any provisions for algorithmic accountability?

The European General Data Protection Regulation (GDPR) separately addressed automated/algorithmic decision-making. Data subjects have rights like notification, access and objection if subjected to pureplay automated decisions. The Indian Bill, however, does not draw such a distinction – data under the Bill definitionally includes that which is processed by automated means. The Bill includes general accountability and transparency provisions such as those around categories of personal data collected, manner of collection, purpose of processing, data principal rights and process of exercise of rights, right to complain against platform to the relevant authority, trust scores, and information on cross border transfers. However, most of the operative processes around this will emerge under delegated legislation.

Data portability is the only provision where a data subject has an expressly stated right in respect of automated processing – data subjects have the right to receive (and have transferred to any other data fiduciary/platform) their personal data in a structured, commonly used and machine-readable format where processing is conducted through automated means. This includes personal data that users provided to the platform, as well any other information generated about them, or which forms part of their profiles.

While there is no GDPR-esque algorithmic accountability under the Bill (around the facets of decision-making, etc.), slivers of hope emanate from provisions on privacy by design, transparency requirements and accountability provisions generally applicable regardless of the means of processing. Much like data protection impact assessments, it would be helpful if subsequently created regulations under the Bill also create a framework for algorithmic impact assessments, as are being envisaged pursuant to the right to an explanation in the regime in the EU.

Conclusion

The majority of the profiles on matrimonial websites appear to be operated by family members of the person seeking to get married. While some of these platforms obliquely make the registrant responsible for obtaining the requisite consents from the relevant person, I'd be curious to find out how many actually take permission appropriately. In a lighter vein, and now that I've completed writing this, perhaps I'll direct my family friends to these matrimonial websites — I'm sure they'll receive far better assistance in the matter of the match than I could ever provide!

*

Kriti Trehan is a Partner at the Law Offices of Panag & Babu. She leads the technology laws and policy advisory practice. She works across a wide range of issues in the technology sector, where regulatory frameworks are still

evolving. She counsels innovators on strategy and compliance on offerings untested by Indian law. In recent times, Kriti has engaged closely with industry and regulatory stakeholders on privacy, data protection, platform immunity, localisation, next generation networks, access, net neutrality and sectoral regulation for tech services. She tweets at @krittirehan

Edited by Aditi Agrawal

#NAMA: Looking at how well the Personal Data Protection Bill, 2019, protects user rights

The Personal Data Protection Bill, 2019, was introduced in Parliament in December 2019, and was referred to a 30-member Joint Parliamentary Committee for review. The Bill is the first legislation that focusses on privacy of citizens, and could potentially result in significant overhaul of digital businesses and companies. The Committee is expected to submit its report to the Parliament before the Budget Session concludes on April 3, 2020.

Earlier this month, MediaNama held discussions in Delhi and Bangalore on the main aspects and impact of the Bill with a wide set of stakeholders. The discussions were held with support from Facebook, Google, and STAR India in Delhi, and with support Facebook and Google in Bangalore. The discussions were held under Chatham House Rule, so quotes have not been attributed. Quotes are not verbatim and have been edited for clarity and brevity. Read our full coverage of the discussions here: #NAMA India's Data Protection Law – January 2020.

The following is Part II of our notes from the session on user rights and data fiduciaries, read Part I here.

Does the Bill do enough for user rights? Does it live up to Puttaswamy standards?

It's a good thing that right to erasure is there, the rest maintains the status quo as the 2018 Bill, said a speaker. It's commendable that most rights under the Bill are the same as the ones in GDPR. It boils down to how regulations around the functions of the Adjudicating Officer would work, a speaker said.

The Bill is all right when it comes to private companies, but not when it comes to protecting users from the government, according to multiple people:

- “**Individuals should have been allowed to make complaints and carry out legal proceedings, rather than leaving it to the DPA.** This was a similar issue with Aadhaar, where only the UIDAI could decide what complaints to take up. The Bill is all right in terms of rights, but the large carveouts made for government, the data localisation business, and critical personal data may have to be tested again in a court of law. The Bill complies with the Puttaswamy standards, **but not when it comes to government exemptions.**”
- “The Bill fares well with respect to private companies to ensure individual rights. **But it fails in respect of protecting individual rights vis-à-vis the State.** The blanket exception to processing data without consent for state functions is extremely troubling. A law cannot be based on

exceptions, it has to be based on rule, and exceptions have to be granted *in exceptional situations.*”

One of the problem areas in the Bill is the excessive distinction and hierarchy between the state/government as data fiduciaries and the private players as data fiduciaries, said another speaker.

Using ambiguity to the government’s benefit

According to a lawyer, **Section 35 appears to be “drafted very cleverly”** and **“there might just be enough for it to by-and-large be constitutional.** It’s worrying that the government has access to that kind of information, and the power to exempt itself to such a large extent,” they said.

“At the same time, the law has beautiful qualifying words. For instance, ‘necessary or expedient’. But we have no idea what is necessary or expedient because there is no jurisprudence. The grounds on which they are talking are the same as the ones in Puttaswamy, or the Constitution under which any fundamental right can be restricted, such as ‘may, by order’, ‘notify in writing’, direct at this law shall not apply to any central, to any particular agency.”

An audience member pointed out that “it’s a serious problem that the Bill is government heavy, and not user-heavy. The DPA’s job is to mediate between users, government, and industry, but it doesn’t have enough structure to be able to that.”

Does the Bill protect users from private entities?

Yes, according to one speaker: “It doesn’t get better than this when you look at privacy law internationally, including GDPR.”

- “A lot of detail will come through in the DPA’s delegated legislation, which is why it’s important an open consultative process, and conversation with industry to understand best practices in cyber-security and encryption for example,” said a speaker.
- The Bill is progressive as far as you exclude the government exemptions portions of it. It’s like an iceberg at this time, the DPA’s regulations will define the rest, said another speaker. “Agency can be given to the user such that they have the ability to pursue action against bad actors,” they added.
- “There might be some regulatory capture of the DPA, because the eligibility criteria of the DPA’s members has been diluted to bits. It’s unclear to what extent the DPA will be open to suggestions from consumers and consumer advocates,” said another speaker.

How would data portability be operationalised? How would it impact companies' intellectual property?

Right to data portability is the a user right under Bill, but there is a concern that it would impact intellectual property of private companies, according to a lawyer with expertise in intellectual property rights.

“While right to data portability is a fair right, how would the line between data generated about me versus data generated about me using proprietary algorithm be drawn?” asked another speaker. “It’s a company’s entire business model and intellectual property. How would we ensure that technology companies are not penalised for using their proprietary materials on user data?” they queried. According to another speaker, the Bill is cognizant of this, as it specifically mentions that the only exception to the rule about data portability is if it impacts trade secrets, which has a higher threshold than copyright.

“Whatever I create in a machine-readable form will not just be a compilation, but some intellectual input will go into it; and companies will necessarily create something proprietary, and that can be protected under the Copyright Act. This is the data which companies have competitive advantage on, and the trade secrets exemption is not enough,” another speaker highlighted. Besides, right to data portability may also infringe on another person’s personal data privacy, noted a participant.

How does right to data portability safeguard data of other users? Does it account for their consent?

An audience member asked how the bill would deal with a situation where a user porting their data is also pulling their entire social graph which has other users’ data, even possibly sensitive personal data, along with their own. How would the new platform deal with this, since they haven’t taken the consent of the other users, the audience member asked.

“The language in the Bill creates this challenge,” said a lawyer in response. “If data portability were to be associated only with data that I have provided the platform by myself and that data had to be ported, it wouldn’t really be an issue. However, now the platform has to port data it received from me, but also information *associated* with my profile, as well as any data *it has generated about me*.” The Bill doesn’t solve for this yet, the lawyer concluded. Another speaker said that it remains to be seen how consent would be dealt with in this situation:

“GDPR has a provision on how entities are required to deal with data that they did not get access to directly from the user themselves, but that’s absent from this Bill, but this question should definitely be posed to the regulator as to how rights of ancillary users protected.”

How will portability work between industries, since there isn’t standardisation?

One can port data from telco to telco, but how can one port data from Orkut to a hospital or telco?, asked a audience member.

Again, “the Bill doesn’t envisage this, although that’s what a user is more likely to do”, the Bill says the fiduciary has to make user data available to them in a commonly used and machine-readable format. “But it doesn’t say anything about whether two telecom operators, or two social media companies should be able to access it. It’s sector and industry agnostic. The Bill envisages, in spirit and principle, that a user has to be empowered enough to take their information from one platform to the other,” said the speaker.

Would right to data portability apply to eKYC?

There are already provisions for a central KYC repository, said a lawyer who has worked on financial services.

“So if I open an account with ICICI Bank, and do my KYC with ICICI Bank, the bank has to deposit that information with CERSAI. Later if I want to open an account with IDBI, I just have to quote one number, a KIN number, then IDBI Bank can access my KYC data from that central repository,” the lawyer said. “This is also incorporated by the RBI and its master directions on KYC,” the lawyer concluded.

Dealing with data breaches

It’s unfortunate that the DPA will decide whether or not to notify a data breach to data principals, and that the data fiduciary has to take its permission, said an audience member. But the reason for this may be to ensure that a notification may be to balance bad actors from taking advantage of a breach, said a speaker. “In any case, the DPA is holding our rights in confidence, but it’s ability to do so is doubtful,” the speaker said.

From what some members of the Joint Parliamentary Committee have been saying, “the delayed notification means the company has to tell the customer about a breach, when the DPA believes that you must, but the company can always tell the customer in the interim.”

Why the central government deciding what’s sensitive personal data is an issue: An audience member said they found it “considerably troubling that you [the government] decides what is sensitive data for me”. “A person of a religious affiliation may not want anybody to know what kind of movies they are watching, for example. Some people like to show off where they travel to, others for security reasons may not want that to be known,” they said. And this why “any data breach, any disclosure should be notified to whoever the data belongs to, by default. So, we should not get into the trap of what is sensitive and what is non-sensitive,’ the person said. The Bill allows the Central government to notify other kids of data as sensitive personal data in addition to the 11 listed categories.

Other issues

DISHA to stay? The Health Ministry said a month ago that it's scrapping DISHA because discussions on health data will be subsumed within the Personal Data Protection Bill. DISHA will go, but the larger principle on sectoral regulators will very much continue to be in place.

Porting health data in emergencies: Prime facie, an individual has the right to access all their information, and in cases of emergencies, one hospital can request another hospital for information. Let's say X Hospital has my data and I'm now going to Y Hospital in an emergency, X Hospital now no longer requires my consent if it is an emergency situation to transfer that data to Y Hospital. The PDP Bill is a sector-agnostic principle-based bill, so sector-specific regulation may be created by the Health Ministry at a later stage.

Conflict with Digital Health Blueprint: "The National Digital Health Blueprint is a purely technical document, but talks about electronic health records, sharing of electronic health records, setting up a new authority that's going to oversee this entire framework, so on and so forth. It talks of the user owning their data, but the Bill has no such concept of ownership. The Blueprint talks of about data being owned by the patient for their lifetime, but per the Bill, users can erase their data, so they are totally at conflict. If the principal legislation says you can erase data and the other legislation or the subordinate one wants data to be preserved for the lifetime of a person and longer, there's a fundamental conflict," an audience member said.

Scope for self-regulation: The DPA can choose to recognise codes of practices, including those by industry, to be part of the regulations. The Authority will prescribe the codes of practice. Any scope for self-regulation or industry participation will be at the level of stakeholders interacting with the DPA.

What's lawful processing under the Bill? What is lawful processing would be a combination principles such as free and fair processing, principles around transparency and data minimization, etc, and then on the consent-based framework, and ways of data collection, etcetera.

Is a missed call campaign by a political party. Can a missed call qualify as consent? Are political parties data fiduciaries? A missed call is a grey area, but it would not qualify as consent, since consent has to be free, fair, transparent, among other things, per the Bill. The user has to very clearly know why their data is being used, how will it be processed, what are the probably significant consequences and harms. The Bill also says that inferred consent is not explicit consent.

Read more: *Personal Data Protection Bill, 2019: Looking at social media intermediaries and significant data fiduciaries*

What can be better

Our speakers recommended the following steps to make the Bill better in terms of protecting user rights:

- **Clear, specific, transparent regulation:**
 - There should be clear and specific regulations from the DPA.
 - There should be a transparent process for delegated legislation where businesses and start-ups can get involved. There should be an open consultative process, white-paper approach each time the DPA makes one of the 40 decisions under the Bill.
- **Specify DPA's powers:** The Bill should also lay out detailed manuals the DPA's executive process on licensing and investigation. For example, the US has a 1,275-page document and SoP on how to investigate banks; the RBI has no manual, which means it can literally do anything it wants to do.
- **Engage with industry on non-personal data:** The requirement for requisitioning of non-personal data can be improved by creating a procedure for engagement, wherein a data fiduciary may respond to such a request, either to clarify its stance regarding feasibility or for any objection it may have. Currently, there is a specific requirement for compliance with all directions of the DPA, which is highly and heavily influenced by the Central government.

*Read Part I of our notes from the session on user rights and data fiduciaries here.
Read our coverage of the discussions here: #NAMA – India's Data Protection Law – January 2020.*

#NAMA: Impact of Personal Data Protection Bill, 2019, on companies

The Personal Data Protection Bill, 2019, was introduced in Parliament in December 2019, and was referred to a 30-member Joint Parliamentary Committee for review. The Bill is the first legislation that focusses on privacy of citizens, and could potentially result in significant overhaul of digital businesses and companies. The Committee is expected to submit its report to the Parliament before the Budget Session concludes on April 3, 2020.

Earlier this month, MediaNama held discussions in Delhi and Bangalore on the main aspects and impact of the Bill with a wide set of stakeholders. The discussions were held with support from Facebook, Google, and STAR India in Delhi, and with support Facebook and Google in Bangalore. The discussions were held under Chatham House Rule, so quotes have not been attributed. Quotes are not verbatim and have been edited for clarity and brevity. Read our full coverage of the discussions here: #NAMA India's Data Protection Law – January 2020.

The following is Part I of our notes from the session on user rights and data fiduciaries, read Part II here.

What will be the impact of the Bill on companies? How difficult will compliance be?

Being India's first comprehensive data protection legislation, the Bill is going to have a fundamental impact, said a speaker. "The current law, the IT Act, places limited obligations on companies, and only regulates sensitive personal information. With the new law, companies will have to overhaul operations, reconsider business practices, think through their plans, strategies, and the way they are using data," the speaker noted.

Compliance would have to be done in three categories, another speaker explained:

- Basic housekeeping, such as whether companies have the right security practices, purpose limitation, storage limitation, etc.
- Securing user rights such as data portability, right to erasure, etc.
- Compliance by significant data fiduciaries, including preparing impact assessment reports, which will be a disproportionate burden on the significant data fiduciary, and which the Data Protection Authority (DPA) will play a role in.

On the role of the DPA, the speaker pointed out that the regulator "has to make decisions on at least 40 and probably significantly more aspects of the Bill,

ranging from user requests, whether companies can charge a fee, anonymisation standards, etc. These rules will affect start-ups and determine compliance cost. The challenge will be how to ensure that the rules are framed in a transparent, consultative manner”.

What kind of compliance time frame can companies expect?

Depends on size, activity, scale, etc.: Since the bill will come into effect in phases, different activities will be affected at different stages. The duration companies will need for compliance depends on the scale of their operations, how complicated their data flows are, how much data they are collecting, how many different countries they are operating in, how much sensitive personal data they are dealing with, etc.

Some businesses have said that six months is all they need. “Companies who are already compliant with GDPR, may be already compliant with the Bill to a large extent, although not in some critical aspects.”

‘Data is the new oil’: “The nature of our Bill is fundamentally different, since our Bill is only in part a Data Protection Bill, it’s also a ‘data is oil’ bill, which makes it a little more difficult to comply with.”

Depends on DPA: “A lot also depends on the DPA’s regulations and its classification of companies as significant data fiduciaries. It’s unclear what companies can substantively do about it right now.”

Not much that companies can do until regulations come: “Companies can start thinking about and considering the Bill, but they can’t do much until the delegated legislation under it emerges. The Bill is strictly principle-based and companies don’t exactly know how to begin compliance. The practice-related aspects on how to locate data in certain jurisdictions, the compliance processes for data collecting, processing, storing, etc, how verifications would be operationalised will only become clear later.”

But companies can apply the best-in-industry practices to hedge their bets. “A good step would be if the industry playing an active role once the DPA, and be active in figuring out the regulations, practices, and standards it will set. For instance, a regulation on encryption or anonymisation should ideally say ‘do best available’, or do ‘best-in-industry standards’ as opposed to prescriptive directives from the DPA.”

Industry associations will have to be proactive, and bring in codes that work for companies. Since the DPA members also aren’t needed to be experts in data protection, it would be a good idea for industry to get together and decide best practices.”

Dealing with privacy-by-design policy certification

The definition of the privacy-by-design policy in the Bill is quite open-ended as it talks about operational and managerial policies, as well as technical standards, pointed out a speaker. “Organisations will have to develop privacy programs, and then they can ask the DPA to certify each and every organisation’s privacy programme. This will be extremely cumbersome for the DPA,” the speaker said. Under the Bill, every data fiduciary has to have a privacy-by-design policy, but not everyone has to submit it to the Authority, noted another speaker.

Although such certification exists under GDPR as well, “it’s voluntary and organisations choose to get their certifications because it looks good for them”. Moreover, the burden for certification “is on outside certifying agencies, and not the regulator,” the first speaker added.

How the policy has to be formed, and the time frame for submission, will be determined by the DPA’s regulations. **“Even with this, there’s too much discretion with the DPA. It could say that everyone has to submit the policies or may it could ask only select fiduciaries to submit it. Again, there’s no transparency around how it will arrive at that decision,”** pointed out a participant.

How is it different from the ‘Data Trust Score’? Under the Bill, an auditor will give an organisation a ‘data trust score’, and the data fiduciary is supposed to put it in their privacy policies. The same requirement exists for the certifying privacy-by-design policy. The only apparent difference between them is that data audits will be conducted annually, but the privacy-by-design-policy certification will happen if companies make changes in their privacy program over the course of their certification period.

Regulating social media intermediaries: why?

Why are they in a ‘data protection’ bill? “The inclusion of “social media intermediary” has come out of nowhere,” a speaker said. The government has been trying to regulate social media entities for a while, and it has been inserting regulatory provisions for those companies in whatever legislation it can, the speaker continued. Another speaker asked if it has anything to do with data protection: “This comes from the issue of traceability in the courts. It seems to be something that is being done under the guise of data protection,” the speaker said.

The verification requirement is ironic: Although a data protection act is meant to ensure that organisations don’t have more personal data than required, the verification requirement unnecessarily ensures that social media companies will have access to sensitive personal data, the speaker highlighted. “You’re just giving them an additional, very crucial data point to actually have more accurate profiling and surveillance, which doesn’t fall into the objectives,” the

person said. According to another speaker, “an easier and smarter solution would be to allow verification of messages rather than people.”

And it's difficult to implement: According to a lawyer, the verification requirement will be challenging with regard to children, since the Bill requires that their age be verified, and parental or guardian consent needs to be taken. “The child user may claim to be a certain age, but there is no way to make sure that's that is actually their age,” they explained.

It also compounds the regulatory problem: “In India, regulators suffer from the problem that their mandate is not clearly defined,” pointed out a speaker, adding that “until 2016, it was never specified what is the RBI's job is.”

“Similarly, the DPA's job is data protection, but the government is trying to bring in countering misinformation into the same Bill. In the process, you end up creating an authority or regulator whose mandate is not clear and so they have a lot more discretion than they otherwise would,” a speaker said.

Additionally, since the DPA isn't independent, “it essentially creates a very unaccountable structure, which allows the government to do a whole bunch of different things without necessarily sticking to the mandate of this bill.”

What's a consent manager? What could it look like? How does the Bill regulate it?

The closest parallel to a consent manager would be the NBFC Account Aggregator framework, said a lawyer. The idea germinated in the Justice Srikrishna Committee report's idea of a ‘consent dashboard’, noted a speaker. Under the Bill, consent managers will be a new category of entities, and they will be data fiduciaries, and will be in control of an individual's personal information, will be able to make decisions about that information, said a speaker. Other speakers had several other guesses about what a consent manager could be and do:

- The consent manager would be a third-party service that allows a user to bring all their applications on the same service, and define which application has access to which category of data for which purpose, for how long, what are the retention periods, how can it be stored, etc. The user may be able to manage their rights under the Bill — some of which are rights to confirmation, access, erasure — via the consent manager.
- The consent manager could be like a wealth manager, that is, a trusted expert to manage user consent. Or it could go the Account Aggregator route, which would make it a one-stop shop to view all your permissions in one place, make it easier for different business to go to one entity and get access, pull whatever information the user wants from that one entity as opposed to going and talking to 35 different entities, and so on.

- The reason it's a data fiduciary is because it will have user's personal data, such as the email address, and which platforms it's associated with, perhaps the user's age, phone number, etc. Therefore, it becomes a data fiduciary since it independently also has access to user information, and also has access to the user's information from other platforms.

One of the speakers, who is also a lawyer, said consent managers look "wonderful on paper", and even the Srikrishna Committee said they were a good idea, based on the Account Aggregators framework. The Committee had observed that:

- One method for managing consent is to ensure that every data fiduciary has their own consent dashboard.
- The second is to have a centralised dashboard, which is what the 2019 Bill suggests. The Committee had said that this method would have serious issues regarding interoperability, because one can't even imagine how many data fiduciaries take a user's consent throughout the day. So operationalising this will be slightly problematic.
 - Another method, to solve this problem, is for data fiduciaries to have their own consent dashboards and move on to a centralised dashboard over time. Again that would give rise to questions such as, "who is going to regulate these consent managers, right? Is it going to be sector specific? Is the data protection authority going to regulate all the consent managers?"

Is a consent manager a good idea?

Consent managers have worked fairly well for businesses and reduce the scope of a business slipping up and opening themselves up to liability, said a participant whose company has invested in consent managers outside of India. "Pilot results we have funded show that no matter what you do with privacy policies, people will not understand it. You simplify it, you put it in Hindi, nobody is going to understand it. It doesn't affect people's behavior and understanding, which is why consent managers are an interesting idea," the person said.

At the same, it might be concerning that "a brand-new concept has been introduced in a primary legislation, when it hasn't been sufficiently stress-tested elsewhere," another participant said. The speaker noted that the the RBI's Account Aggregator framework — the closest parallel to the proposed consent managers — took years to take off. "Although the regulatory framework went live in 2016, MeitY came up with electronic consent artefact, which the RBI then adopted. *Then* the RBI put out regulations saying that Account Aggregators need to function in user interest, that they're just a pipeline, an intermediary. They can't collect consent and pass it on, it just sits in the middle to makes the user's life easier," the speaker highlighted.

Another speaker was much more cynical: "But it's worth thinking as to why would a user put all their data in one place, or give access to all their data to

one data fiduciary? It's like putting all your money in one bank. What if the bank gets robbed?"

Do we really need it? How can it be better?

Maybe not. But maybe we need more clarification.

"Deleting it from the Bill might be as such as bad idea," said the speaker who pointed out the issues with Account Aggregator framework. Another speaker said, "It's too unclear if consent manager will just be a pipeline. It may actually be holding user information in escrow for other companies or platforms." And if this is the case, "then having a certification, protection, clarificatory framework on the dos and don'ts of a consent manager would be helpful," the speaker said. Another speaker also highlighted the concerns with a manager, and how its activities could be restricted:

"Maybe more specifics, such as protective frameworks, could come through sectoral regulations, as the RBI has done with AA — such as who can and cannot be AAs, what they can do, meeting the net worth limit. Is the manager just meant to be a conduit for managing consents, will the user do their own analysis? If you give consents to say for X amount of time to Y companies of a certain category, can the companies use the data to cross-sell certain or advertise certain products to you?"

What about consent managers being significant data fiduciaries?

There are several models that companies can follow, a speaker said, taking the example of a UK-based consent manager, which is both the data manager and consent manager. "This consent manager manages the data on behalf of the consumer and stores it in different places. In that case, the company would be a very, very significant data fiduciary." But there are also lighter models "where the manager is just a pipeline, and doesn't handle storage. So the extent to which a consent manager will be a data fiduciary depends on the DPA's regulations on who qualifies as a consent manager and who needs to register." Another concern is that if a third-party — the consent manager — is managing the user's consent, the company would also need to know where their liability ends, and the manager's liability begins.

How would companies' intellectual property rights be affected by government access to non-personal data?

The non-personal data is a huge deviation from the 2018 Bill, which had said that there should be a separate legislation for non-personal data, said one of the speakers. "This is the exactly where the 'data is oil' aspect comes in, pointed out another speaker. "Just as oil found on private land is not private, but is the State's, the argument here is also that data belongs to the government, and it can take it over. This is a very problematic way to look at non-personal data."

“The scope of non-personal data is very large, there’s a lot of data gathering companies do, and the information give them competitive advantage over others. Will corporations continue to invest in developing this kind of data and analytics, only to part with it when the government asks for it? This will definitely stifle innovation.” — a speaker

Read Part II of our notes from the session on user rights and data fiduciaries here. Read our coverage of the discussions here: #NAMA – India’s Data Protection Law – January 2020.

#NAMA: Issues around surveillance in the Personal Data Protection Bill, 2019

The Personal Data Protection Bill, 2019, was introduced in Parliament in December 2019, and was referred to a 30-member Joint Parliamentary Committee for review. The Bill is the first legislation that focusses on privacy of citizens, and could potentially result in significant overhaul of digital businesses and companies. The Committee is expected to submit its report to the Parliament before the Budget Session concludes on April 3, 2020.

Earlier this month, MediaNama held discussions in Delhi and Bangalore on the main aspects and impact of the Bill with a wide set of stakeholders. The discussions were held with support from Facebook, Google, and STAR India in Delhi, and with support from Facebook and Google in Bangalore. The discussions were held under Chatham House Rule, so quotes have not been attributed. Quotes are not verbatim and have been edited for clarity and brevity. Read our full coverage of the discussions here: #NAMA India's Data Protection Law – January 2020.

The following is Part I of our notes from the session on government access to data, read Part II here.

“The Puttaswamy judgement and the discourse around data protection in India arose in the context of Aadhaar, where the State was seen as the chief privacy violator. The Personal Data Protection Bill was an opportunity to correct that, but the State wants to exempt itself from all the obligations instead,” a speaker said.

Sections 35 and Section 36 emerged as the crux of issues of the Bill as they grant government agencies too much power with respect to processing citizens’ personal data. Section 35 empowers the central government to exempt any government agency from the provisions of the Act for purposes of public order, national security, etc. Under Section 36, certain provisions of the Bill are not applicable for purposes of law enforcement, and court orders.

The State needs to be a model actor given the asymmetry of power between State and citizen: Unlike data that is collected by private companies such as Facebook, it is more concerning when the State does it, a speaker said. **This is because the State has the power of law behind it and a monopoly over violence.** “**The State is the only actor that is sanctioned to commit violence or force of law, in a way private actors cannot,**” they explained. As a result, centralisation of power in the State can make citizens vulnerable to extreme harassment, blackmail or coercion, they said.

CHAPTER VIII

EXEMPTIONS

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 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.

30 *Explanation.*—For the purposes of this section,—

(i) the term "cognizable offence" means the offence as defined in clause (c) of section 2 of the Code of Criminal Procedure, 1973;

(ii) the expression "processing of such personal data" includes sharing by or sharing with such agency of the Government by any data fiduciary, data processor or data principal.

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—

- (a) personal data is processed in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of any law for the time being in force;
- (b) disclosure of personal data is necessary for enforcing any legal right or claim, seeking any relief, defending any charge, opposing any claim, or obtaining any legal advice from an advocate in any impending legal proceeding;
- (c) processing of personal data by any court or tribunal in India is necessary for the exercise of any judicial function;
- (d) personal data is processed by a natural person for any personal or domestic purpose, except where such processing involves disclosure to the public, or is undertaken in connection with any professional or commercial activity; or
- (e) processing of personal data is necessary for or relevant to a journalistic purpose, by any person and is in compliance with any code of ethics issued by the Press Council of India, or by any media self-regulatory organisation.

Personal Data Protection Bill, 2019 – Section 36

2019 Bill widens government's powers and exemptions

“The 2018 version of the Bill said that processing of personal data by the State for security of the state is exempt from most obligations provided that it is in accordance with law, is necessary, and is proportionate. So the classic proportionality elements, mandated by *Puttaswamy* were introduced. Those in itself were not adequate and the Bill had not gone far enough to address structural and procedural elements, or embed safeguards for this type of access,” a panelist explained.

Proportionality standard: The *Puttaswamy* judgement established that the right to privacy can be curtailed only if it passes the four-fold proportionality standard, that is, it gave

1. Legitimate state aim

2. Legal basis in law
3. Least restrictive means used
4. No disproportionate impact on the right holder

The 2019 Bill, the speaker continued, reduced the already inadequate safeguards on government exemptions even further. This is problematic because:

- **Agency-specific exemption rather than function-specific:** The government can now exempt *entire agencies* from *all* provisions of the Bill, irrespective of whether it is performing the function of security, the speaker said.
- **Increased number of reasons for granting exemption to agencies:** Earlier, the exemption could be granted only for national security reasons, but now four more grounds have been added — sovereignty, integrity, friendly relations, and public order. “While these grounds have a constitutional basis in Article 19(2), this is still a widening of what the 2018 Bill said, something that needs to be examined,” they said.
- **Government agencies can be exempted from all provisions of the Bill:** “The 2018 Bill was narrowly tailored wherein even State agencies that accessed personal data for security of state had to deploy security measures, process it in a fair and reasonable manner, and be regulated by the DPA,” they said. In the 2019 Bill, it means that the exempted agencies would not be regulated by the DPA.

“Is the removal of *all* privacy safeguards the least restrictive way, as set forth by the *Puttaswamy* test, to justify the blanket exemption for an agency? Does it justify the wholesale exemption for, say, the Bangalore police to collect *everybody’s* data without *any* application of the safeguards in this Bill?” — a speaker in Bangalore

- **Exemption for government from all offences:** Under Section 35, in effect, the government is exempted from the Offences chapter as well, a speaker pointed out, unlike the 2018 Bill. “Even if we find the government guilty of something, there is effectively no statutory remedy,” they said.
- **‘Reasoned’ order is enough to exempt an agency:** The speaker highlighted that now the central government would only need a ‘reasoned’ order to exempt an agency as opposed to a legal/statutory mandate.
- **Lack of oversight over law enforcement agencies:** Section 36 allows the central government to exempt law enforcement agencies from certain provisions of the Bill for law enforcement purposes, a speaker said. As a result, while oversight by DPA and need for security safeguards remain, two safeguards that were there in the 2018 Bill have been removed, a speaker pointed out.
- **Removal of statutory basis for surveillance by intelligence agencies:** The 2018 Bill explicitly said that for law and order situations, you need a statute or law passed by the Parliament, a panelist said. This would have made it mandatory for the Parliament to actually deliberate on these issues before they exempted an agency. That has been done away

with in the latest draft.

- **Rights of victims, witnesses and suspects have been diluted as proportionality is undermined:** The 2018 Bill allowed law enforcement agencies to process data of a victim or a witness or a person related to a crime or offence that the agency was actively investigating or seeking to prevent, a speaker said. Agencies also had a limitation for how long such records could be kept. Now, it for general prevention and prosecution of offences and contraventions of law, and purpose limitation and limiting retention of data have been scrapped. Proportionality has been removed as a statutory obligation.

One panelist disagreed and said that **the 2019 Bill is an upgrade** as under the 2018 Bill, government agencies could process data without consent for any function of the state. But in the 2019 Bill, this non-consensual processing is limited to providing targeted benefits and certification.

Does the Bill pass muster of the proportionality standards?

Puttaswamy standards of necessity and proportionality are not part of a statute: “Irrespective of that the State or the courts say, a regulator goes by the law. The regulator doesn’t go by the precedent set in judgements,” a speaker said. As a result, the requirements of necessity and proportionality should be a part of the act itself. This is visible in the case of sedition, a lawyer explained, wherein the police goes by the text of Section 124(A) of the IPC, which is very broad, instead of the Supreme Court judgement that *read down* the section and said that there has to be an incitement to violence.

Looking at the Pegasus scooping scandal: “Installation of malware on somebody’s phone for the purposes of surveillance does not have any legal basis. It conforms to no legitimate state aim, and is overly broad. The manner in which surveillance is carried out in India, and its institutional architecture, in my opinion, is completely and manifestly unconstitutional. Steps such as the Central Monitoring System, NATGRID, would not meet the proportionality standard at all.” — a speaker

Some definitions are too broad under the bill: A number of terms in Section 35, such as “security of the State” and “public order”, are very vague and have not been narrowly defined. “In a statute, you have to be much more precise; you can’t have broad value statement like you have in the Constitution,” a speaker said. “Public order” is a “term of wide latitude” that has been used for a lot of things, especially to impose Section 144 of the CrPC, remarked another speaker. “When use of administration or discretionary power is tailored so broadly, it inevitably provides a scope for misuse,” a speaker said.

- **Delegating powers to private actors for public order?** “When the exemption allows you to take any measure to ensure safety of or provide

assistance or services to any individual during any disaster or any breakdown of public order, apart from the State, it also gives power to a person to determine what is a public order situation and then without consent process your data or seek your data. So, it's a very wide provision," a speaker argued. Letting private individuals determine when they can process personal data without consent when they see a breakdown of public order is a "disaster", another speaker said.

- **Does contravention of law include contractual breach?** Under Section 36, certain agencies of the State can be exempted for contraventions of law. "This is not just criminal offence or cognizable offence. It can even be a contractual breach," a speaker said. This is a really wide power that law enforcement agencies, and State agencies in general, will get.

Standards of proportionality are undermined by security of the State:

"In terms of application of the Bill, it means that an agency like the Delhi Police can be exempted from all provisions of the Bill, citing security of the State or public order," a speaker said. They further said that while this could be challenged in court and the government would have to prove that the step is proportionate, it was unlikely to happen. "Anybody who is a long time observer of Indian jurisprudence around national security would say that our courts have been extremely reluctant in seeking accountability or embedding safeguards on or limiting the national security exception," they said.

However, a speaker disagreed with this assessment and said that a nine-judge bench of the Supreme Court held that proportionality standards, which includes the standard of necessity, must be adhered to for any data processing and collection by the State. "**This has been subsequently reaffirmed and recast in different scenarios by the Aadhaar bench, the internet shutdowns order in Kashmir, and by the Bombay High Court in the Vinit Kumar v. CBI case,**" they explained.

Lessons from the Vinit Kumar v. CBI case: The Bombay High Court interpreted Section 5(2) of the Telegraph Act in light of the Puttaswamy judgement and actually ordered the destruction of evidence that was collected through surveillance since it did not comply with the parameters of the Telegraph Act. The Court concluded that evidence obtained unconstitutionally was not admissible in court. It applied the proportionality standards to the surveillance order and concluded that CBI didn't pass muster:

1. **Legal basis:** Public safety and emergency are very high standards. In this case, it was a question of corruption, and thus the surveillance was violative of Section 5(2) of the Telegraph Act and of Rule 419(A) of the Telegraph Rules.
2. **Least restrictive means:** The orders were overly broad and were thus not specific or proportional.

Lack of transparency and accountability for government agencies

Lack of Parliamentary or judicial oversight: “There is a big gaping hole in the PDP Bill as it doesn’t talk about judicial or parliamentary oversight; it doesn’t even actually have a review committee,” bemoaned a speaker. Even under the *PUCL* judgement, the Telegraph Act, 1885, and the Information Technology Act, 2000, there is executive level oversight and a review committee that looks at all the decisions made about surveillance, they explained. A lawyer said that the rights to privacy judgement established that you need some semblance of oversight to give right to privacy its full meaning. Petitions challenging Section 5(2) of the Telegraph Act and Section 69 of the Information Technology Act are already pending before the Supreme Court as they don’t mandate judicial or Parliamentary oversight, as directed by the Puttaswamy judgement.

Lack of transparency in the rule-making process: According to the PDP Bill, 2019, all safeguards and procedural obligations will be laid down by the regulator, that is, the Data Protection Authority, through a notification. This, as a speaker highlighted, means that there is no debate in the Parliament about these. Unlike the sections of the Bill which will be discussed in the Parliament, the rules and regulations, which will *actually* govern how the provisions are notified, will not be subjected to a debate. “Like the Aadhaar Act, much of what is laid down comes through regulations and is not laid down in the Act itself, and that is concerning,” they said.

The Bill tries to create legal basis for private access to Aadhaar. A speaker explained that when Aadhaar was made mandatory for KYC for banks, the Supreme Court struck it down as it would not have been proportionate. However, the new Aadhaar amendments created a backdoor to the judgement because of which the amendments are now being challenged in the Supreme Court, they said. **“Sections of the PDP Bill effectively try to retrofit the Aadhaar ecosystem under the garb of public services.** They now want to include all private players in the Aadhaar ecosystem to be protected/given immunity under the Bill,” they said.

A speaker went so far as to say that UIDAI doesn’t even need to be exempted under Section 35 or Section 36 as the Bill has been written in a way “to accommodate Aadhaar’s incursions into privacy”. However, another speaker said that commercial use of data collected for state purposes has been struck down as unconstitutional, citing the Supreme Court striking down Section 57 of the Aadhaar Act. They argued that this will still largely be the case.

Read Part II of our notes on government access to data here. Read our coverage of the discussions here: #NAMA – India’s Data Protection Law – January 2020.

#NAMA: Improving the Personal Data Protection Bill, 2019, to safeguard against surveillance

The Personal Data Protection Bill, 2019, was introduced in Parliament in December 2019, and was referred to a 30-member Joint Parliamentary Committee for review. The Bill is the first legislation that focusses on privacy of citizens, and could potentially result in significant overhaul of digital businesses and companies. The Committee is expected to submit its report to the Parliament before the Budget Session concludes on April 3, 2020.

Earlier this month, MediaNama held discussions in Delhi and Bangalore on the main aspects and impact of the Bill with a wide set of stakeholders. The discussions were held with support from Facebook, Google, and STAR India in Delhi, and with support from Facebook and Google in Bangalore. The discussions were held under Chatham House Rule, so quotes have not been attributed. Quotes are not verbatim and have been edited for clarity and brevity. Read our full coverage of the discussions here: #NAMA India's Data Protection Law – January 2020.

The following is Part II of our notes from the session on government access to data. Read Part I here.

Potential safeguards against surveillance in the Bill

There are potentially two safeguards against broad surveillance and unwarranted government access to data as given under Section 36, according to a speaker:

1. **Section 4** [Prohibition of processing of personal data except for “specific, clear and lawful purpose”]: Section 36 does not exempt the operation Section 4. The requirement for clarity and specificity might obviate some of the broadness that comes with this kind of surveillance.
2. **Section 92** [Bar on processing certain forms of biometric data]: This section prohibits the processing of biometric information except when permitted by law. There are very few statutes that explicitly authorise the processing of biometric information — Aadhaar Act and Identification of Prisoners Act, 1920 that permits people to be fingerprinted when a person is arrested.
However, if the exemption is granted under Section 35, that’s a “wholesale exemption” which is a more difficult situation, they clarified.
3. **DPA is crucial to curtailing government access to data:** According to the Bill, government agencies are also data fiduciaries and have responsibilities that a data fiduciary would have. But they can be relieved of most, if not all, of their duties through exemptions under Section 35 and Section 36. However, a speaker pointed out that this would be governed by the efficacy of the Data Protection Authority (DPA). “With this Bill,

we have vested all our faith in the DPA to keep us safe from any privacy violation. But if the DPA itself is ineffective or compromised, nothing will work,” a speaker said.

DPA’s functioning would be determined by how independent it is, but under the latest draft, it is executive committee. Unlike the 2018 Bill, there are no judicial members. As a result, the DPA will effectively be controlled by the government, and thus its effectiveness remains a fundamental question, the speaker said. But, as a speaker pointed out, “the whole point is that the central government is the first violator”.

“We saw this happen with the Cyber Appellate Tribunal under the IT Act. When one of the chairpersons retired, the government did not appoint any one new and just kept the post vacant. And thus the Tribunal became essentially non-functioning.” — a speaker

Greater oversight over access, curtail exemptions: Recommendations

- 1. Make the objective and preamble of the Bill unequivocally about data protection:** “The Preamble of the Bill needs to unequivocally state that it is for the enforcement of administration of the right to privacy of all individuals. The digital economy equivocation has to go. How would we feel if the Domestic Violence Act said that it is meant ‘to prevent violence against women and to preserve family values’,” a panelist railed.
- 2. State should be the model data controller:** The Statement of Objectives of the Bill should say that the State will be the model data controller. Also, a speaker said that the term ‘data fiduciary’ has to go as it deprives users of their agency. “Data controller is a much better functional term,” they offered.
- 3. Judicial review of access to personal data by government agencies:** Just as the Srikrishna Committee had recommended in its report, there should be prior judicial review of State access of personal data. “This can be done through a designated court or judicial members in an independent authority such as the DPA,” proposed a speaker. This includes an appeal mechanism against the decisions of this judicial body, and ex-ante and ex-post reporting mechanisms.
- 4. Oversight mechanisms to make State agencies accountable:** “Oversight bodies should be identified which monitor the working of State agencies,” a speaker said. Such bodies should release periodic reports with details about the functioning of these agencies, data fiduciaries which constantly get requests for personal data, and the number of requests they receive.
- 5. Amend the Bill to curtail exemptions under Section 35:** When it comes to inclusion of four more grounds to blanket exemption for agencies under Section 35, speakers generally opposed the move and said that the

Bill needs to be amended to define terms such as ‘national security’, ‘public order’ narrowly.

6. **Notify users:** Deferred notice should be sent to data subjects, a panelist said. “This should be followed by right to redress,” they said. There should also be a means to notify the user if there is any kind of unlawful surveillance, another speaker proposed, both by the private companies and by the State.
7. **Evidence from surveillance that was not a proportionate response be inadmissible:** Taking a leaf out of the Bombay High Court judgement on evidence collected from disproportionate surveillance, a speaker suggested that information that is obtained from surveillance which does not conform to the proportionality standard of the Supreme Court should be decreed unconstitutional and not be admitted in court.
8. **Appoint Data Protection Officer for State agencies:** “Law enforcement agencies and agencies accessing this kind of personal data should have a data protection officer which goes through interception warrants and data requests, and make sure that they adhere to the law, and have least restrictive measures,” a panelist suggested.
9. **Need for whistleblower protection:** Although whistleblower protection was not discussed by the Justice Srikrishna Committee, it is required in light of revelations about the NSO Group-Pegasus scandal where it is clear that a government agency purchased it, but its identity remains unknown, a panelist said. “We have a Whistleblower Protection Act, but it has not been brought into force, and even that does not do enough,” they argued.
10. **Have a separate law to implement surveillance reform:** “We need a separate law that gives intelligence agencies a statutory basis for their existence itself,” a speaker said.

Read Part II and Part III of our notes on government access to data. Read our coverage of the discussions here: #NAMA – India’s Data Protection Law – January 2020.

#NAMA: Data Protection Authority's independence and powers under the Personal Data Protection Bill 2019

The Personal Data Protection Bill, 2019, was introduced in Parliament in December 2019, and was referred to a 30-member Joint Parliamentary Committee for review. The Bill is the first legislation that focusses on privacy of citizens, and could potentially result in significant overhaul of digital businesses and companies. The Committee is expected to submit its report to the Parliament before the Budget Session concludes on April 3, 2020.

Earlier this month, MediaNama held discussions in Delhi and Bangalore on the main aspects and impact of the Bill with a wide set of stakeholders. The discussions were held with support from Facebook, Google, and STAR India in Delhi, and with support from Facebook and Google in Bangalore. The discussions were held under Chatham House Rule, so quotes have not been attributed. Quotes are not verbatim and have been edited for clarity and brevity. Read our full coverage of the discussions here: #NAMA India's Data Protection Law – January 2020.

The following is Part I of our notes from the session on data protection authority. Read Part II here.

DPA's independence: why, how much, and what now?

The DPA's independence is crucial given that its core functioning includes regulating government bodies, not just private entities, pointed out a speaker. In fact, what's unique about the DPA is the degree to which it will have to contend with the State as an antagonist, said another speaker. This is not the case with the Competition Commission of India (CCI) or with the Insolvency & Bankruptcy Board (IBB), s/he added.

How independent is the DPA currently?

The current selection committee consists of a cabinet secretary, secretary of legal affairs, and MeitY secretary. According to one of the speakers, this makes it a "government committee and an in-house affair". The speaker pointed out that this is a deviation not just from the 2018 draft, but from many other Indian laws and regulatory setups. "The CCI allows external experts on the selection committee, who suggest names for vacancies, although the government appoints the members. Even the IBB allows outside experts," the speaker said.

When asked about how independent the DPA is, our speakers made the following points:

- **The DPA's independence falls short** structurally given the kind of shadow that the Central government casts on the working of this body, in

terms of budgetary controls and the power to make directions. But it also falls short functionally; we don't know the DPA's processes, transaction of business; what they will be left to the rules, so we will have to see what they are.

- **The DPA is certainly less independent and less transparent, when compared to TRAI.** Regulators that have come after TRAI have gone further steps, while the TRAI Act only says that TRAI has to transparent in functioning, other regulators such as the Airports Authority of India, and the IBB have gone a step further and have said that they need to consult the public. The PDP Bill only does this for codes of conduct where it says the DPA needs to consult the public, stakeholders, and even other regulators, but it doesn't say anything for the other regulations.
- **What we can learn from TRAI:** A lot of TRAI's ability to be somewhat independent is because the public is involved with its functioning; people send in comments, all stakeholders feel they have a say and an opportunity to oppose. So when TRAI wants to take an independent stand, it can say that a certain stakeholder is saying so.
- **There is a divestment of powers from the DPA, and an investment of those powers in the Central government.** This points to an intent to politicise data protection and to make critical decisions relating to users and companies' political decisions. This goes against a global trend and it's something to worry about.

Another speaker disagreed stating that while the DPA's level of independence under the current bill is a cause of concern, "**that doesn't mean it's doomed for failure**". "We should also look at how the DPA would build up its reputation for independence. Even with its current structure, it may be able to stand up to the government, or may annoy the government; that may still show independence," the speaker said.

Piping in on the general disagreement, one of the speakers warned that data issues are being increasingly politicised in India, but also globally. "Power is taken away from expert regulators and given to governments and legislatures who are not trained to handle them. This might be because the value of data is becoming increasingly clear, or because international trade negotiations, or other reasons – but none of this spells any benefit for users."

We don't have an ideal regulator, let's start afresh

Do we have an effective DPA anywhere in the world? It's too early to comment given that the world is still grappling with the GDPR, and each country has their own way of regulating personal data, said a speaker, citing that "while GDPR adopts a more generalist approach, Australia and the US have tilt towards sectoral regulators".

"If we want to think of an ideal regulator, we need to search outside of what exists, especially in India," said another speaker. "People have admitted in courts that

no regulator passes the muster, in cases where constitution of tribunals and other agencies have been challenged in the Supreme Court. We are much better served in not looking at precedent and starting afresh, and think about the objectives we want to meet and how we would get there.”

Where did all our regulators come from? What insights do they give into the DPA?

“Independent regulators came about as the private sector came into the picture” and functions shifted from state monopoly to the private sector, explained a speaker. “Apart from making sure that the industry behaves, regulatory agencies started to need technical experts with domain knowledge, and those from outside the bureaucratic setup,” The private sector’s development gave rise to the need for independent regulatory agencies “which could both operate at arm’s length from the government and have technical expertise. The broad objective was to regulate market failures and to have an oversight mechanism,” said the speaker.

There are three constituencies the DPA is going to have to mediate or at least cater to: the government, the private sector, and individuals and users, ordinary citizens, which is probably the most important constituency.

The accepted wisdom currently is that the DPA is going to be a market regulator, pointed out a speaker. “We haven’t been able to solve what the role of a market regulator is, and is still an open question. Our best market regulators haven’t successfully mediated between the competing interests of these three constituencies. Besides, market regulators by themselves are relatively new, they aren’t more than 20-30 years old, and before that commissions or government-created agencies that were meant to exercise expert jurisdiction over a particular issue did so primarily to protect the interests of users,” the speaker said.

There are now two kinds of market regulators, one which have greater powers over their markets such as SEBI and TRAI, and the other kind which shares powers with the central government. But “we don’t know which route the DPA will go”.

The issue with India’s market regulators: There is a challenge pending in the Supreme Court around the constitutionality of the CCI, which would be baseline for what a constitutionally compatible regulator should look like. The case is being argued on a separation-of-powers plank, the idea being that regulator is a delegate of the State’s power.

The CCI case in the Supreme Court reflects that an issue with today’s market regulators: that the new-age regulator of the post-1990s is an extremely hybrid body that investigates, prosecutes, decides disputes, sets standards, makes laws at two levels — for everyone, and for specific actors — it’s way too hybrid.

“Given this, how are you going to control that the DPA functions efficiently, and that the laws it framed are enforced with rigour?” the speaker asked.

In fact several speakers pointed out that the Bill envisions a dual function and objective of the DPA — to protect user privacy and also to promote economic growth, goals which seem to be inherently in conflict. As one speaker pointed out in Delhi, this is like drafting a law against domestic violence against women, the objectives of which are to prevent such violence, but preserve family values at the same time. Our speakers weighed in on this:

- This regulator should have a one-point agenda: the commitment the government made to the court that it will protect privacy by this law. “This law has one objective only and that is to maximise privacy,” said a speaker.
- Another speaker disagreed, stating that the DPA’s objective doesn’t have to be either. “I think there is a nuanced way in which both can live together, both can thrive together. I guess the moral of the story is data is capable of economic growth either way. It’s up to us to do that in a privacy-centric manner.”
- Seal DPA from other courts: “We also need to seal the regulator from the judiciary, not just from the government. For instance, the Patents Act has a compulsory licensing power that asks a judge, not a market regulator, to have regard to certain principles when applying his power, and one of principles is the general benefit of India. Should it be a court duty to protect a country’s interest? **This is a larger question of cleavage in laws in all developing economies, but this is not the duty of the regulator, their duty is to protect the market and users in the market.”**

DPA’s powers and functions

Is the DPA being asked to do too much, or too little?

It’s being asked to do a lot, and it’s good that the DPA’s roles have been narrowed down previous draft, where it had to carry out 26 functions. Now it has to carry out 14 functions, the speaker said, reminding everyone that “being India’s first Data Protection Authority, it will have to lay a lot of the groundwork for future sectoral regulations to follow suit”.

Should it be up to the whims of the DPA chair to choose whether to toe the government line or not? Isn’t it risky? “We take that risk all the time with every regulator,” one speaker declared, going on to explain the following:

- **There’s always risk of regulatory capture:** An existing regulator, whose appointment process is supposedly well-structured – the Chief Vigilance commissioner. The CVC is appointed by the Prime Minister or Finance Minister, and the Leader of Opposition – the idea being why

should the government have monopoly over this appointment. But we still see in CVC who are effectively non-functional.

- **We will simply have to see how much of a public-facing role the DPA will have in its functioning.** TRAI invites public comments, takes people's suggestions, CCI holds its hearings.
- **A DPA cannot just be this body which sits and makes its regulations,** rules and policies, and so on. That's ripe for capture, and regulatory capture can be done by the government, private entities, or by vested interests. You prevent capture, not just by robustness, but also by subjecting it to public scrutiny.

What should the DPA prioritise? The DPA has an adjudicatory function, a legislative function (drafting the regulations), an executive function (enforcing the regulations), and an advisory function (making recommendations to the government). The DPA will have to prioritize what it has to do on Day 1, on Day 365, Day 3650.

On Day 1, they should start with making the regulations and maybe handle some of the disputes according to one speaker. Agreeing with this, another speaker said that the DPA should set down norms on Day 1, since it's going to "form the basis for industry practice". An audience member said that while "the regulator doesn't need to say the regulation it will draft each month, it can give a roadmap and logical explanation around it".

Should the complaints redressal function be separate from the DPA's other functions?

Not necessarily, instead primary problem is how to get the *right complaints* before the DPA, according to one speaker. This includes what access users have when they've suffered a privacy violation, and what procedural and substantive safeguards do they have.

Yes, absolutely, complaints redressal should be separate. "Our [entity redacted] submission ever since the white-paper came out was that the law should create two agencies, one the DPA, and another called the Data Protection Redress Agency, an ombudsman-like scheme whose only job is to carry out the specialized function of complaints redressal. It's a very different function from regulation making." The speaker added that there's also a potential conflict of interest, if one body is doing both functions:

"If a lot of complaints are coming on some issue, it could mean that the industry is performing badly, but it could also mean that the regulator is doing really bad supervision and regulation. If the regulator is responsible for both, its incentives could be to downplay complaints that point to the flaws in their own regulatory system. It's important to have someone else looking at complaints the regulator should not be controlling both process."

Maybe not. The DPA needs to take some time, the RBI could do it because its experienced: Other regulators do have an complaints body or adjudicating wing: the RBI has created an Ombudsman for consumer complaints, while RERA, SEBI, and CCI have an adjudicatory division, pointed out another speaker. “But it would be better that at least in the first few years — until the law is stable and clear — to not have a separate complaints body. Otherwise, there is a risk of the Ombudsman becoming a little to *panchayati*, and the user won’t know whether he’s going to get relief, and nobody would know if what the DPA or possible complaints body is doing is in accordance with the law and regulation,” the speaker said, adding that:

For instance, the RBI has got years and years and years of practice for what can and should not be done. So it makes sense for the RBI Ombudsman to direct banks to do or not do something. We may want an ombudsman later on depending on how you know, the DPA handles disputes and how the DPA balances all its functions.

Read Part II of our notes on the Data Protection Authority here. Read our coverage of the discussions here: #NAMA – India’s Data Protection Law – January 2020.

#NAMA: The Data Protection Authority's capacity and composition, and recommendations on how the regulator should work

The Personal Data Protection Bill, 2019, was introduced in Parliament in December 2019, and was referred to a 30-member Joint Parliamentary Committee for review. The Bill is the first legislation that focusses on privacy of citizens, and could potentially result in significant overhaul of digital businesses and companies. The Committee is expected to submit its report to the Parliament before the Budget Session concludes on April 3, 2020.

Earlier this month, MediaNama held discussions in Delhi and Bangalore on the main aspects and impact of the Bill with a wide set of stakeholders. The discussions were held with support from Facebook, Google, and STAR India in Delhi, and with support from Facebook and Google in Bangalore. The discussions were held under Chatham House Rule, so quotes have not been attributed. Quotes are not verbatim and have been edited for clarity and brevity. Read our full coverage of the discussions here: #NAMA India's Data Protection Law – January 2020.

The following is Part II of our notes from the session on data protection authority. Read Part I here.

Does the DPA have the necessary capacity? Can it regulate for 1.3 billion people?

An audience member pointed out that while other regulators like SEBI and RBI deal with only limited entities, the DPA's regulated entities cut across sectors, and are many more. So will the DPA have this capacity, what does history tell us?

Regulation for a population is only indirect: Taking the example of an existing regulator, a speaker pointed out that SEBI regulates listed entities, even though those impacted by it could be half the country's population, whoever holds shares or has invested in mutual funds, etc. SEBI is not trying to solve every one person's problem, they're only concerned with the entities that they are regulating.

There won't be a flood of complaints, there's a natural barrier to access: Even though users can go to the DPA with complaints, but it still doesn't mean that existing regulators such as the CCI has to set up an office in every last taluk and district. There is a natural barrier to access, only somebody who has the resources and ability to make a complaint will make one. The DPA is not going to be flooded by too many complaints, because it requires certain high level of knowledge and resources to even make a complaint to the DPA.

Finally, a speaker pointed out that, it "can't be the DPA's job to

keep everyone who comes to it happy" and we will have to wait and watch the further regulations that the DPA drafts, which will be the "real meat and bones of this regime".

Users can always go to the High courts and Supreme Court: If the DPA does not act on a user complaint, the user can approach the High courts and Supreme Court, both of which are Constitution rights and cannot be curtailed by any law. **The bill only restricts users from approaching a civil courts** regarding matters that come under the Appellate Tribunal's matters. Users will have to exhaust the remedy they have under the bill, but they can always approach the higher courts.

Should there be state-level DPAs?

It could be worth considering, **but you could have four equally incompetent DPAs, and that may be worse.** "I don't know if there's any regulator that has successfully managed to address the fact that they have to regulate for the 1.3 billion people, or if they regulate for the immediate body of influencers, companies, and government bodies that surround them," said a speaker.

Yes, but that ship has sailed: "I've always maintained that every state needs its own data protection authority in India, and the bill should have allowed for this" said another speaker in disagreement. "The Bill leaves very little space for the state to take any different or independent view. If Karnataka government said that, 'this is too onerous, our start-up sector is going to die. We want to come up with a better data protection regime for startups located in Karnataka' — they can't do that."

On government exemptions under the bill

According to a lawyer and public policy professional, the exemption to the government is not a blanket exemption; "it's fairly wide-ranging, and also specific and fairly limited; individual applications of that power can and will be challenged". If Section 35 — which allows for exemptions to government agencies — was giving an exemption to too wide a set of government bodies, that could have been challenged, the speaker said, "but if Section 35 is challenged in its current form, the court could say that the *Puttaswamy* principles were never not absolute and there were always restrictions".

- Rather, each restriction on privacy — or exemption given to each government agency — will be tested on its own merits. It's difficult to judge whether or not the government should have any overall exemption powers, because that's a very difficult framework to answer this question. But it can be tested for each exemption."

The interaction between central government and DPA is crucial when it comes to the requirement to share non-personal data, and on cross-border

data flows in that the central government has the power to decide any country as adequate, the speaker further added that:

“This is lifted from the GDPR under which the European commission (arguably) has the power to decide adequacy. But the provision under Section 34 does say that the government will consult the authority and then deem another country adequate for cross-border data flows. It’s important for the DPA to lay down exactly how far it will have a say in what the central government does in its sovereign powers.”

What kind of people should the DPA consist of? Who should lead it?

Unfortunately, there’s a tendency in government to pick government servants, although the Supreme Court has been trying to convince them not to do that, explained a speaker.

Private sector people or within government? “Initially, it will be very difficult to get a person from the private sector to set up the DPA, it will be somebody from government. What the government has tried with having Raghuram Rajan as the RBI governor, that is, somebody from the outside – should be applied across regulators, the DPA should also do this. The government usually an individual who is a good administrator, and another individual who is an expert. But it’s possible to find somebody who can meet both these requirements, the government just does not exercise its imagination often enough,” the speaker added.

How about retired judges? “We should just stop putting retired judges in any official government post. It’s destroying the judiciary, and destroys the post also,” one of the speakers declared.

Who should it be? It needs to be someone with a mix of administrative experience and substantive merits of it. Say somebody who has been say head of tech company in India or somebody who has worked at a very high level who understands the business practices. In a field like this where the practice is changing on a day-to-day basis, you can’t expect that somebody who has had like hoary administrative experience will be able to respond in a day-to-day basis.

The DPA is ripe for setting the practice that regulators can come from the private sector, we shouldn’t just be looking for retired or serving bureaucrats. For the initial years, the agency will have to have government servants for work to be set up, but over a period of time, it will be healthy to get private sector people to be part of this regulator.

DPA and other sectoral regulators: the bill tries to talk a little bit about it and process around that, “but it’s going to be a big battle on things which are already in place because that the voluntary MOU between regulators that the bill refers to is not even mandatory, which in my view should have been,” said a speaker.

Recommendations on DPA's functions, structure, and practices

On DPA's powers, structure, functioning:

1. **Bring back the structure of the DPA as in the 2018 draft. Divest the government's powers, and reinvest them in the DPA.**
2. **Have some part-time members:** The DPA only has full-time members, but part-time members can bring technical and external expertise. India has regulators with both structures, and there also needs to be a review of which design works better. Under its law, TRAI has a chairperson, two whole-time member, two part-time members. “Although I have no internal knowledge of how well the part-time structure works, it has clearly worked for TRAI. TRAI has had part-time members who have been academics and professors,” the speaker explained. The benefit of part-time members is that they are “not too embedded into the system, and the chances of dissent and debate in meetings of the regulator will be higher.”
3. **The selection committee's composition needs to radically change** to have more independent experts, and fewer government nominees.
4. **Some important rules should not be left to the DPA's discretion:** Other decisions which have been left to delegated legislation by the DPA, such as procedures for meetings of the DPA and selection committee, how nominees there will be, how long will they spend on recommending members, will voting process of DPA meetings be public, all of these are too important to be left to the DPA's discretion and need to be embedded into the rules.
5. The bill says that processing of a user's data must be “fair and reasonable”, but the trouble with both these concepts is that they're endlessly litigable, they set no baseline meaning, they don't necessarily direct you to the privacy enhancing outcome or the innovation enhancing outcome, or an outcome that's deferential to the state. It doesn't give any sort of normative, prescriptive, idea. Frame fair and reasonable processing to be more defined, this would foreclose a lot of litigation on what those words mean.
6. **Hive off the adjudicatory and decision-making functions from the others.** If that's not possible, then at least specify the types of procedure this body will follow. It's good to do the specification beforehand rather than, making it up as you go, as some regulators have done.
7. **The DPA should be mindful that data is capable of creating significant economic value,** as data protection authorities across the

world have realized. It's important for this to be reflected in the way cross-border data flows are handled. For instance, portability can be monetized, data breaches can be penalized in such a way that the funds from the penalties go to the DPA and bolster it financially.

8. **The DPA should also not forget that the centre of the Bill is the user and their rights.** State surveillance has often taken centre stage in the bill, even though *Puttaswamy* was clear that no law should sidestep privacy, while enriching the government and leaving the citizen behind. The DPA needs to be mindful of this, especially given Section 91, and the fact that it shares powers only with the Central and not State governments.

Best practices from other regulators that the DPA can adopt

1. **Make consultative process part of the DPA's organisational DNA:** every time the DPA wants to do something on the legislative or advisory front, they should involve the public and specific stakeholders.
2. **Transparency:** The DPA should not wait for anybody to file an RTI, instead it should make the RTI redundant by saying that any question people have is on the website.
3. **Open up hiring:** Too many of our regulators hire almost exclusively from the government or from the geographic area in which they are located. The DPA should be ready, willing, and able to tap the best talent across the country, both at the top and mid levels. It's going to need quality researchers, quality lawyers, and people capable of framing privacy issues properly. A lot of people are happy to offer the government given the kind of importance that the work has, the meaningfulness it has. Maybe the DPA's top official can be a retired bureaucrat for the first two years, but it can try and get outside talent later on, and it would be able to create a much more robust and effective body.

Read Part I of our notes on the Data Protection Authority here. Read our coverage of the discussions here: #NAMA – India's Data Protection Law – January 2020.

#NAMA: Issues with classification of data in the Personal Data Protection Bill, 2019

The Personal Data Protection Bill, 2019, was introduced in Parliament in December 2019, and was referred to a 30-member Joint Parliamentary Committee for review. The Bill is the first legislation that focusses on privacy of citizens, and could potentially result in significant overhaul of digital businesses and companies. The Committee is expected to submit its report to the Parliament before the Budget Session concludes on April 3, 2020.

Earlier this month, MediaNama held discussions in Delhi and Bangalore on the main aspects and impact of the Bill with a wide set of stakeholders. The discussions were held with support from Facebook, Google, and STAR India in Delhi, and with support from Facebook and Google in Bangalore. The discussions were held under Chatham House Rule, so quotes have not been attributed. Quotes are not verbatim and have been edited for clarity and brevity. Read our full coverage of the discussions here: #NAMA India's Data Protection Law – January 2020.

The following is Part II of our notes from the session on cross border data flows, read Part I here.

Classification of data is complex

What can potentially be sensitive personal data: A lot of Indian names can actually reveal the caste of a person, so wouldn't names also be considered sensitive personal information, a speaker asked, and added that there is currently a lot of confusion on what exactly is personal data, and what is sensitive personal data. Another speaker highlighted the problem by giving the example of photographs collected for non-biometric purposes, for instance, for making an album, will those photographs be then considered personal data, or sensitive personal data?

- **Is there anything such as personal data?** From the definition of sensitive personal data, it appears as if there is no such thing as personal data, a lawyer noted. The person explained that if fiduciaries start processing any kind of data with sufficient depth and clarity, it might give away inferences to people's health information, sexual orientation, mental status etc.
- **Definition of personal data is contextual:** Another lawyer said that the definition of personal data in the current Bill is extremely contextual. "There is no possible way that we can create an exhaustive list of personal data, and there is good reason for it: That same data packet could be personal data in one context and not in another context. So this entire exercise of data segregation itself is extremely difficult," they noted.

What is really the objective behind this data classification exercise, a lawyer

asked. “So, sensitive personal data has to be localised, does that have an objective? Maybe, it is due to the fact that certain data types might need a heightened sense of security. However, to provide that security to localised data, it will have to be encrypted. With the entire section on government exceptions, it appears as if it wants to access some of that data. But, will it be possible when that data is encrypted?” the person said.

What about critical personal data? A person in the audience said that as a small business, they are very anxious over the uncertainty of collecting critical personal data since it hasn’t been defined in the Bill. A speaker noted:

“Critical personal data hasn’t been defined in the Bill, and neither does it have a basis for classification. Neither does the Bill doesn’t spell out any process by which critical personal data is going to be defined, nor will it involve the Data Protection Authority or the industry in the classification process. I don’t know how we are even going to arrive at any business predictability around that.”

What falls under financial information? Financial service providers need to collect people’s names to provide them with financial services, will those names also be categorised as sensitive personal data, a person asked. “There is a lot of ambiguity in the way sensitive personal data has been classified in the current Bill,” they added.

- Another speaker noted that the reason why financial data was classified under sensitive personal data is to comply with the RBI’s data localisation mandate. “This classification legitimises the RBI directive and the clarification that came later on, which specifically said financial data has to be stored only in India, can be processed outside the country and deleted in some time and that’s exactly how sensitive personal data under this new Bill is treated as well,” the person added.

Illustrating the problem with the classification of sensitive personal data, with respect to processing it outside India, a lawyer said:

“Imagine I email you my bank statement, which by definition is sensitive personal data because it has my financial data. Then in the next email I also send you a cat meme. In which world will a data fiduciary be able to save the financial data part of the email in India and process it outside while the cat meme can go anywhere in the world?” — a lawyer

“Just the semantics of this condition are so new that even the best data protection team in the world would not be able to decode it,” the same person said. They also highlighted that only because personal data has been allowed to be processed outside India, doesn’t mean that it isn’t of much worth to businesses. “A lot of email providers actually process users’ emails and attachments in order to target advertisements better. This processing largely happens on the server,” the person said.

How payments services will be affected: A lot of people store their credit card information, bank passwords on browsers which have a sync service. This means that if these people use their browser outside India, the stored data just gets synced to that particular browser instance, and is never generally stored on the server, a person explained. However, the classification of sensitive personal data with respect to processing outside India would mean that the same data fiduciary will have to consider those instances differently in different countries, which would essentially break the service, the person explained.

- The first speaker also said that just putting in place the architecture to segregate sensitive personal data from current datasets is going to be an egregious task, more so for industries that are just starting out, since they'll have to invest heavily in establishing this architecture. "This will create a bottleneck in their operations," the person added.

Health data being made part of sensitive personal data can also become a problem, a person said, and explained: "A lot of people come to India from around the world to get treated for certain health conditions, and hospitals here can also serve these people remotely. Similarly, what would happen if Indians travelling to other countries have to visit a hospital there unexpectedly which requires their health data? Will the current localisation norms for health data not affect that?"

- To that, a lawyer responded by saying that health data being part of sensitive personal data should not be looked at from the perspective of data localisation alone. Instead, we should discuss having separate laws that deal with the transfer of certain kinds of data, for instance, the Health Insurance Portability and Accountability Act (HIPAA) in the US, the person added. They also said that we should not bat to remove certain kinds of data from the bracket of sensitive personal data, just because localising that would be a deterrent.

Read more: Personal Data Protection Bill, 2019: Considering data localisation and its effects on payments

Adequacy vs. data localisation: Which is the better approach?

Adequacy is better: Adequacy under EU's GDPR, is an indirect form of localisation, without any of the categorisation problems in the Personal Data Protection Bill, a speaker said. "It means you can either process data in a particular country, or not process it there at all, which makes compliance much easier," a lawyer said. Even though India doesn't have adequate status with the European Union yet, it is still possible for people in India to access someone's computer in the EU remotely, because technically, the processing is still happening in the EU, the person added. Another speaker noted that adequacy

is a better way of dealing with overseas processing of data, simply because data localisation will be unenforceable.

“The reason why the EU chose adequacy over data localisation was because they did not want to get into an unsolvable problem.” — a lawyer

If the EU says that its citizens’ data can go to another country, only then can that data be taken overseas. Also, that data would enjoy the same level of protection as in the EU, and companies will have similar legal liabilities to ensure that that data remains safe and secure, another person added.

- If India were to choose ten countries where it would be fine to process Indians’ health and financial data, none of the problems we have discussed thus far will arise. Most data fiduciaries will be happier to follow adequacy procedures than the localisation mandate, they added.
- A speaker pointed out that while adequacy is a much better option than data localisation, it still has its own share of problems, including the fact that it is an extremely bureaucratic exercise.

“When you open the Xiaomi Home app, it actually asks users on which server they want their account to be on. The options that pop up include India, China and the USA. What Xiaomi is doing at this point in time is basically giving users the ability to choose where they want their data to be stored and processed,” a lawyer said, explaining what the adequacy procedure would look like.

Will India get adequacy under GDPR?

No. “With the current provisions in the bill, it’s impossible to see how we would get adequacy status under GDPR,” a lawyer said, and explained: There is a provision in the Data Protection Bill which says that data of non-Indians, when processed in India, might not enjoy the same level of protection that the Bill offers. This can be a potential hindrance in India getting adequacy status with the EU.

- With the kind of surveillance norms we have in India, along with the section of the Data Protection Bill which talks about government exceptions, India will not get adequacy with the EU, another person said. “Getting adequacy is a long process, and it takes a lot of negotiation with the EU to get adequacy. Our Bill won’t give us enough power to negotiate with the EU,” the person added.
- The section which deals with the restriction on cross border data flow in the PDP Bill, 2019, doesn’t make it clear if it also applies to data of foreign nationals. Does that mean that even their sensitive personal data will have to be localised in India? If that were to happen, India will fail all adequacy requirements, a speaker said.

Read Part I of our notes on cross-border data flow here. Read our coverage of the discussions here: #NAMA – India's Data Protection Law – January 2020.

#NAMA: Issues with data localisation norms in the Personal Data Protection Bill, 2019

The Personal Data Protection Bill, 2019, was introduced in Parliament in December 2019, and was referred to a 30-member Joint Parliamentary Committee for review. The Bill is the first legislation that focuses on privacy of citizens, and could potentially result in significant overhaul of digital businesses and companies. The Committee is expected to submit its report to the Parliament before the Budget Session concludes on April 3, 2020.

Earlier this month, MediaNama held discussions in Delhi and Bangalore on the main aspects and impact of the Bill with a wide set of stakeholders. The discussions were held with support from Facebook, Google, and STAR India in Delhi, and with support from Facebook and Google in Bangalore. The discussions were held under Chatham House Rule, so quotes have not been attributed. Quotes are not verbatim and have been edited for clarity and brevity. Read our full coverage of the discussions here: #NAMA India's Data Protection Law – January 2020.

The following is Part I of our notes from the session on cross border data flows, read Part II here.

Data localisation in the 2019 Bill: Not really an improvement

The data localisation norms under the current Bill are **not an improvement** over the Srikrishna Committee's draft bill, said a speaker.

Segregation of data by type is very tricky: “The datasets that we work with might be a mix of personal data, sensitive personal data, and maybe even critical personal data. But the data localisation or data mirroring requirement would be applicable to the whole data set, and it makes no sense for us to scrub and segregate personal data from it to send it outside India,” the person added.

Mirroring of sensitive personal data in India would be challenging, because implementing mirroring standards and infrastructure would be difficult, another speaker said. The list of sensitive personal data includes things like caste, tribe, political inclinations and religious beliefs, and to extricate all such information from datasets would be a “nightmare,” the person added. Illustrating the challenge in mirroring sensitive personal data, the speaker said: “Imagine a YouTube video where someone has commented about the Citizenship Amendment Act protests; that definitely is a political opinion, which would now have to be mirrored in India. It’s an extremely difficult exercise”.

- **Why even mirror?** If the data is about consumer protection, all transfers would have to be approved by the Data Protection Authority (DPA), businesses will be under strict contractual clauses by virtue of being part

of intra-group schemes, a person said. The person asked that if the transfer of sensitive personal data is going to be so heavily regulated, what is the need to mirror it in India in the first place?

Ensuring segregation and localisation will be an issue: Ensuring that data fiduciaries have localised relevant data would require for someone to look at how networks are designed, how data flows between data centres take place etc., the first speaker said. Highlighting the problems with enforcing data localisation, the speaker added, "you just have to say I have done it [data localisation], and here are three possible sources of evidence. But, in reality, there are maybe a hundred different ways in which data can still keep going outside the country because of how hard it is to perform localisation along with segregation".

- **The economics don't work:** There is also an economic element that might make enforcing data localisation a problem, several speakers concurred. "The most popular cloud service provider in the world lets people choose where they want their data to be processed and stored. If a user selects India to process their data, several services such as AI/ML, APIs are no longer available, and moreover, they will have to pay a price to perform the processing in India," a speaker said, highlighting the cost element behind data localisation.

It's about government access: The draft e-commerce policy had a protectionist intent, in a way that the concept of protecting Indians' data went beyond the idea of privacy. Similarly, the proposed changes to the intermediary guidelines, which require 24-hour communication with the government, show us that there is a regulatory intent for ensuring that Indians' data remains readily available and accessible to the government. That intent is going to find an expression through the data localisation norms in the current Bill, a lawyer explained.

Seeking consent might be a problem for data processors: While getting explicit consent can be easy for data fiduciaries, it becomes a problem for data processors who do not have a touch point with data subjects, a person explained. "As a data processor, when you are using the data for Big Data analytics, pattern generation, risk analysis, and don't have a touch point with data subjects, you will wonder if you can take data out India and combine it with other datasets to identify, for instance, frauds, terrorism risks," the speaker said.

Good that personal data doesn't have to be localised: All speakers concurred that the fact that personal data can be taken outside India was a welcome addition to the 2019 Bill.

Food for thought: can users choose to store their data outside India? "At a global tech summit, Justice Srikrishna was asked if citizens can exercise their right to privacy and ask for their data to be stored outside of India. He replied that he would have to go back and think about this," a speaker narrated.

Data localisation is not about privacy or the economy

Given the types of data that have been categorised under sensitive personal data, such as financial data, it appears as if privacy has become a basic argument under which many other agendas get pushed through, a person noted. Privacy can not be a key argument for data localisation, they added.

Is it about the economy then? Several speakers concurred that data localisation's economic argument falls flat, simply because how can one leverage data stored within India, when the same data is also protected under a privacy law. "The economic argument often made in favour of data localisation is completely false, because you have a privacy regime, nobody is going to access the data to that end, since there is a purpose limitation, collection limitation and storage limitation. If I'm collecting and storing data in India, I'm not going to give it up since I have to also be compliant under the privacy law," a lawyer said.

- If it is about access to data, then storing the data in an encrypted form would defeat that purpose, another person said.

How effective is seeking explicit consent?

Under the current Bill, sensitive personal data can only be processed outside India, and only with the explicit consent of data principals for such processing. But users may not be able to use all the features of a service, pointed out a speaker. In case a data subject doesn't give explicit consent, their sensitive personal information would not go outside the country; this would mean that the user will either not be able to use a particular service at all, or won't be able to use some features of certain products, a lawyer noted. "So, you won't be able to use some filters on Instagram because processing those filters on your photographs happens all over the world in disaggregated networks for speed. Because of that, you won't be able to use their products. So, you can use a minimal version of the service, but you can't use all the features that are actively available," the person illustrated.

"If half the customers of a company were to give explicit consent to process their sensitive personal data outside India, and the other half did not, what will a business do? Are they supposed to have separate clouds to do the processing of data?" — a speaker asked

Let data controllers do their due diligence: Even the GDPR puts the burden on data controllers to have contractual provisions in place, and carry out their due diligence while taking people's data outside the European Union, a lawyer said. For the purpose of processing data outside of a particular border, the idea of seeking explicit consent from data subjects makes no sense at all, they held.

- Another speaker noted that it would be unfair to expect a data subject to decide what level of encryption should be applied to their data while consenting to process it outside India.

Impact of data localisation on businesses

“Start-ups don’t even know what’s coming at them,” a lawyer said, and added: “I was trying to log into a fitness app, and realised that they actually collect biometric data to mark attendance, and realised that they will have to now localise that data and segregate it from all other data sets they have”. Another speaker said that the localisation norms can absolutely “disrupt” blockchain-based businesses and service.

- A lot of start-ups don’t aim for monetisation from Day 1 of operations, and instead, use collected data to generate insights, customer onboarding and engagement in order to reach to a critical mass level, a person explained. The data localisation norms, thus, are more suited for bigger companies with tested revenue generation models since they will find it easier to comply with them, the speaker added.

Need to re-engineer processes: Both processing and classification of data from different datasets is going to be a painstaking exercise for several companies, a speaker noted. A lot of the companies have been operating under a free flow of data environment, and complying with the new norms would mean that they’ll have to re-engineer a lot of their processes. This might result in a large number of companies to look for ways to keep all their data in India rather than take it outside, the person said, and added that it doesn’t help that we are moving towards a heavily regulated environment where companies need to identify data starting from the collection itself, sort it, categorise it and then decide which data moves elsewhere.

Fears of reciprocity: While a lot of IT companies believe that the current localisation norms are slightly better than before, most of them have “expressed resistance” to the current rules because it puts barriers and they also fear that other countries might put similar barriers on them, a speaker said. “The IT industry fears that they could potentially lose out on international trade as a result,” they added.

- IT service providers are also concerned about the intra-company transfer of data which has to be approved by the DPA, since it’s going to be a major hassle, another person noted. They said that had the Bill allowed for a standard agreement with all clauses mentioned, it would have been much better.

It affects B2B transactions as well: “I started using Trello a few years ago, and I think I won’t be able to use it anymore given that they will have to localise my payments data in India, which in all probability it wouldn’t do given that it’s a small company in San Francisco” an audience member noted. Similarly, small artisans, musicians, businesses would not be able to use cheap and good foreign tools because why would those companies want to invest in developing servers in India, the person said.

Opportunity for larger players: A speaker suggested how bigger companies

can potentially help smaller companies in complying with the localisation norms: “Companies like Apple can come up with a business model where anyone who wants to offer their services using their App Store can pay them an additional fee to purchase Apple’s server space in India”.

What would be an ideal timeframe for data localisation?

GDPR’s two years wasn’t enough: “As of now, I can say that the two years allotted to comply with the GDPR was not enough,” a speaker said. “Even for the companies who are already compliant to the GDPR may need more time, simply because our Bill is very different from the GDPR,” they added. **When the GDPR came into force, it was found that almost 75% of the market was non-compliant**, a lawyer said. This, despite the EU having the Data Protection Directive in 1995, and the various judgements pronounced by the European Court of Justice. As of now, the apprehension is around not having clarity on when everything has to be in place, because when portions of the IT Act were enacted, we had seen how the government made radical changes without giving the market time to adjust to it, the person added.

“Thinking of an adequate timeframe to comply with the localisation norms is a moot exercise, because even if you give companies a hundred years, they will not be able to meet the requirement. Unless they can prove that they have one dedicated data centre in India to comply with the norms, it will be difficult to be sure about it.” — a lawyer

Can data localisation norms be applied retroactively? Businesses might have to seek fresh consent from data subjects to take their data out of India, despite the fact that they might have collected their data before the Bill was tabled, a lawyer explained. They will potentially have to do that because they could be using certain data for a completely different purpose than originally intended, they added.

Recommendations

At least for sensitive personal data, the local storage requirement should be removed, and we can decide about localisation with respect to critical personal data on the basis of how it would be classified, a person said. Other recommendations made by speakers:

1. **Relax data transfer norms:** A lawyer said that If we can’t remove data localisation from the Bill, we should ideally bat for relaxing some of the data transfer conditions, including not having to go to the DPA to get every transfer approved, another person remarked.
2. “All of the advanced data protection legislations in the world, including EU’s GDPR, have no data localisation restrictions at all. They have restrictions on cross border data flows, and I think that’s what we should

stick to,” a lawyer noted.

3. Norms of data transfers in the Personal Data Protection Bill, 2019, are confusing and need to be relaxed.
 4. **Focus on securing cross border transfers:** Restrictions on cross border data flow should be removed, localisation should be removed, and instead, we should focus on safe and secure transfer of data, be it through standards, standard contractual clauses, or adequacy.
 5. **Sectoral regulations:** Instead of having a national law that dictates how localisation would work for everyone, we should leave it to the sectoral regulators to decide what works best for that particular sector.
 6. **Need for a compliance roadmap:** The government should work responsibly and come out with a compliance roadmap, as was laid down in the previous version of the Bill, because without it, the situation would become chaotic.
 7. **Explore global collaboration models** like the global privacy enforcement network (GPEN), so that countries respect each others’ sovereignty while allowing for cross border data flows keeping rights of people in mind. Another user said that we can explore mutual recognition or bilateral agreements to allow for free flow of data outside India.
-

Part II of our notes on cross-border data flow focuses on issues with classification of data, read it here. Read our coverage of the discussions here: #NAMA – India’s Data Protection Law – January 2020.

#NAMA: Is defining non-personal data possible? Is anonymising it a good idea?

The first issue with defining non-personal data as the negative of personal data is that personal data is not in a crystallised form in the Personal Data Protection Bill, 2018, said a speaker at MediaNama's roundtable discussion on non-personal data. The second issue is that segregation of personal and non-personal data is close to impossible as there are mixed data sets in the age of digital markets, IoT and Big data. Citing the Personal Data Protection Bill, 2018, another participant said that non-personal data is “100% of the pie with the personal data removed from it”, as participants deliberated whether or not non-personal data was a viable category to begin with.

(Note: The discussion was held under the Chatham House Rule; quotes have not been attributed to specific people. Quotes are not verbatim and have been edited for clarity and to preserve anonymity. Also note that this discussion took place before the PDP Bill, 2019, was made public.)

What are the problems with defining Non-Personal Data?

All data can be traced back to a granular level: “In the context of GDPR, the moment you put the clause ‘relating to humans’, everything becomes personal data. From that definition, 100% of data is either directly or indirectly linked to human beings,” a speaker said. The issue arises because the Personal Data Protection Bill, 2018, did not define ‘personal data’ adequately, as per the speaker. To this, another speaker said that there was a clear distinction between ‘human data’ and ‘personal data’. “I don’t think we should use the two interchangeably. Human data is anything that is generated by human activities. Personal data is identifiable to individuals,” they clarified. “So when you’re talking about whether a community or a region is producing a certain particular effect, it’s not the same as saying that it is personal data. We can’t use it so interchangeably.” However, they conceded that “all kinds of data sharing which related to human activity can eventually be brought down to granular level of individual human beings.”

We haven’t seen non-personal data in practice: “Much as we try to distinguish between personal and non-personal data, we are not going to be able to because we don’t know what non-personal data look like in practice at scale. This is similar to the discussions we had in 2017 when we tried to define localisation. ... I think it’s best to sort of accept that non-personal data exists and just move on because it is a bounded rationality problem,” a speaker explained. Despite acknowledging the problems with defining non-personal data, another participant said, “Non-personal data is a very real thing right now because there is a committee that is deliberating [on it] and a lot of companies and organisations have already presented before it.”

Source of data unknown: “We don’t know where it emanates from, whose

data it is, who is the producer of the data. When I take a cab, am I the one producing data or a cab aggregator?” a speaker pointed out.

Non-personal data as a concept is continuously evolving: The previous speaker continued, “The definition of non-personal data needs to be about limits because arriving at a good definition of non-personal data is going to be tricky and it will constantly be evolving in some ways. So is true for regulation. It needs to be about limits and not about an exact definition.”

Can anonymous data always be traced back to the source?

A number of speakers pointed out that **non-personal data may technically not be possible as the process of anonymisation is not absolute.** “A lot of this data would be the anonymised data and the standard for anonymisation in the PDP bill is an irreversible standard which at this point is not an achievable standard per se. So that automatically creates a lot of confusion in terms of which anonymised non-personal data will be outside the ambit of the PDP bill [2018],” a participant said.

One participant argued that **even if it is not a perfect technique, anonymisation is a useful, functional method.** “Re-anonymisation is possible. So anonymisation is not a perfect construct, but it is a utilitarian concept. That’s a political decision that we want to make [whether we want to anonymise or not]. Even census data to a large extent can absolutely be re-identified. Does that mean that we do not publish census information any longer? It doesn’t, right? Anonymisation can’t be seen as a black and white kind of [concept]. It’s a very much a utilitarian concept, and we have to place those political boundaries,” a speaker said. Another speaker pointed out that there are different grades of anonymisation techniques available, and it’s up to us how we utilise them.

But even anonymised data could eventually be traced back to an individual. “Non-personal data is made out of clusters and something makes those clusters. In the electronic scheme of things, it’s very easy to find out which points make each cluster. Anybody with access to anonymous data can actually come back to the source. There is an electronic trace,” a participant said.

“The government’s understanding [is] that certain kinds of data that is linked to individuals — this doesn’t relate to community data or non-individual data like air pollution data — but this does relate to behavioural patterns, aggregated data can be anonymised. It is very much capable of being reverse-engineered and re-identified. The risk is there and it’s a fairly high risk to take. The assumption that anonymised data — we don’t even know what these anonymisation standards are —, it is safe and is no longer a threat to an individual’s privacy needs to be challenged.”

A participant pointed out that **in certain circumstances, the ability to trace back and de-anonymise data is crucial.** While anonymised medical data can be used keep entire populations safe from diseases, “we should be able

to trace anonymised data back to its origin,” the participant said. “Let’s say my genetic data is out there and there is an outbreak in the market which marks me out for a disease. I should come to know of it,” they said. They suggested that use of data should determine whether or not data should retain “a certain degree of granularity”. This would be determined by law, keeping in mind the risk, they clarified.

Can non-personal data be used to profile groups of people?

Even anonymised non-personal data can be used to profile, persecute, and discriminate against groups of people, some speakers pointed out. At times, de-anonymisation does not even require sophisticated algorithms to target people.

One speaker told us about how political parties send SMSes and videos legally in a geo-fenced area with the help of telecom companies. “Telecom companies will map out the towers that address this geo-fence — without telling the political party the numbers — but they will disclose how many people have latched onto those towers in the last six months, and then allow me to send messages there,” they explained. This kind of service can be paired with other data points — such as mosques in an area through data scraped from Google Maps, or even from the voter roll — and can be used to target potential voters with a lot of specificity. The same means can be used to persecute people.

“Formally speaking, we have a secret ballot system. But when a political party contests elections, their workers always know who voted for them and who didn’t vote for them. This happens because this data is identifiable, it can be narrowed down and correlated with other data points.

“For example, if there is a booth and there are 30 families under it. If a particular political party does very badly, [the party workers] are going to relate it to other things, such as, those families did not come for the rally, or who asked questions when a person went to do their door-to-door campaign, etc. So when correlated with other data, parties always know who did not vote for them, and that is how the political workers ultimately give or deny access to to the politician once they are elected. We will be really kidding ourselves if we think that it is possible to fully anonymise any kind of data.”
— a participant at the discussion

Non-personal data will not be used in silos: A participant explained how the Delhi Police collects two kinds of information about people for their crime maps — their location and their socio-economic information. The latter is collected on a region basis and subsequently used to profile regions as “no data would be used in a silo; it would be used with other identifiers so it would always brand a region”. They pointed out how these methods are used to “red-line” areas and brand areas as “risky” or “not risky”.

Linking databases to distribute government sources: “Even [with] air pollution data, you can say which category of people are creating more pollution, which areas are creating more pollution. You can trace it onto a group of people, say 10 people. How can it not be personal data?” a speaker said. Nikhil Pahwa, editor and founder of MediaNama, pointed out the dangers of linking this data with vehicular data and registration numbers to potentially target people. “If you can trace it [air pollution data] down to an individual, directly or indirectly, it becomes personal data,” another speaker remarked.

“After a point, people will start buying properties where there is less air pollution. You can also imagine lot of things happening with property rates and schools. All nice people living in one location and all ‘bad’ people living in other location. All the government resources will be sent to those nice locations.” — a participant at the discussion

Using health data to profile people: “Let’s say anonymise health data by region. There is this area that has very high incidence of triglycerides (a type of body fat) in people. So you say cholesterol. What is the source of cholesterol? Higher meat eating. Is that a social marker? Is that a cultural marker that interests somebody? When you start thinking down that line, the possibilities are endless and very, very scary,” a speaker said.

Using people’s buying habits against them: “Let’s just say we look at data of women who are buying vibrators online on Amazon, and then we narrow it down to a geographical area and that area comes around to say for example, the area around the university in the city. Then will the women of the university be targeted as being of a loose character?” another participant said.

Data collection for aggregated purposes: “When demographic information is sought in my area, do I have the option of saying that I don’t want things like my religion being used even in an aggregated way? Because aggregated anonymised non-personal data can lead to significant harms. There are examples in Andhra Pradesh and Telangana, where such databases exist and can be analysed very quickly for religion. And you can have gram panchayat-wise percentage of Hindus, Muslims, et cetera. And I think the possible harms there are very, very clear as 1984 and 2002 have shown us.”

- Another person said that during a data collection drive for one of the databases in Haryana, the forms mandatorily asked for caste and religion. Even when this data is aggregated and anonymised, it can still be used to profile groups of people by region.

Read our coverage of the our discussion on Non-Personal Data in Delhi here. The discussion was held in New Delhi on November 28, 2019, with support from Amazon Web Services, Facebook and FTI Consulting.

#NAMA: Considering intellectual property rights over non-personal data

“If it falls under intellectual property, then the government can definitely claim right over such data sets,” declared a lawyer at MediaNama’s roundtable discussion on non-personal data held in November 2019, as participants deliberated if sharing non-personal data, with the government or with other private entities, would infringe on companies’ intellectual property rights.

(Note: The discussion was held under the Chatham House Rule; quotes have not been attributed to specific people. Quotes are not verbatim and have been edited for clarity and to preserve anonymity. Also note that this discussion took place before the PDP Bill, 2019, was made public.)

Is data ownership a useful concept?

Defining property rights over data: A speaker explained that ownership does not automatically translate into private property ownership and thus defining ownership becomes critical. “What are the rights? Is it the right of access? Are we worried about integrity of the data? Is our focus entirely on NPD [non-personal data] in the context of free flow? That if it is not proprietary, then technically we would want it to be through an open API available to all in a machine-readable format,” they said.

- A lawyer said, “It is not data per se that we have to look at in terms of ownership, but the manner in which the data is going to be used, in which it will be monetised, which is where the issues will start cropping up”. Citing the rejection of the ‘hot news’ doctrine by the Delhi High Court, they said that in the case of BCCI, it was not the ownership over the scores per se, but “ownership over the right to monetise the scores”.

IP rights are asserted over databases: A speaker pointed out, “There isn’t really a concept of IP [intellectual property] over a data point; individuals have some proprietary rights over how data is managed, over databases, but not over data itself.” If the aim is to put data in a public commons as a common property for a public good, “there need to be long debates about policy reasoning,” they said.

- **European Parliament’s Database Directive recognises *sui generis* right:** Citing the European Parliament’s Database Directive of 1996, an advocate explained that this allows an entity to have a *sui generis* (in and of itself, independent of other factors) over a database if it has “put in a substantial investment into the collection and creation of the database”. This does not include machine collection of data.

Value of data is derived from aggregation: “Data per se has no value individually; it is only when you collect data and start using it in different databases that value gets added,” said a lawyer at the discussion.

Defining reasons to limit IPR is a must: To limit someone's property rights, you need to have clear and distinctive reasons for doing so; it is only after that that you can move to questions of risk involved, governing usage to protect communities from harm, etc, a speaker said. Another speaker said that regulated entities such as telecom companies already have to give data to the government for certain specific purposes. However, for the government to get access to data to "improve public policy making processes" needs very different kind of arguments because "you are infringing on intellectual property". Before making any policy, all risks associated with it have to be evaluated, and they argued that public good might not be enough of an impetus to warrant that.

However, property rights, not IPR, might be a more useful formulation for protection: One lawyer in the room contested the idea that intellectual property rights protection is the best way of protecting data sets. "If we start looking at IP statutes [copyright, patent] as a means of finding/including data protection, it may not be the right way," they said. However, the basic principles of property per se, that is, the exclusive right to own, to possess, to dispossess something might be a better way to "find a more balanced approach to how this non-personal data should go into a community data set, or should be made available to competitors, and in what manner it should be made available", they said. Looking at the concept of public purpose, voluntary and mandatory acquisition of property by the government for certain purposes, would aid in that.

How the government can access the data it wants to

Indian government can force companies to share protected data sets for public services: Another lawyer in the room explained that under the Indian Copyright Act, "there is a provision called compulsory licensing under which government can force any copyright owner to provide that right and take it away from the copyright owner and use for the purposes it wants". This is when the government believes there is "an overarching public purpose", another advocate explained. On the question of whether the government could force companies to share the data sets, another advocate compared it to the Land Acquisition Act wherein the government can gain control over physical property for public purposes. "If we look at the public purpose for use of a particular data set, then possibly yes, the government can [force companies to share data]," they said.

IPR over data collected by public sensors can also be accessed by the government: With respect to ownership asserted over ambient data collected by sensors and IoT devices in public areas, or instrumentation in smart cities, or by GPS trackers on public transport — all of which serve a public good — the previous lawyer said that "if it can qualify under the level of creativity under Indian law, that is, if there is enough skill applied on it and it results in something which is more than mere law, and has some originality attached to it, it will be enough to get copyright protection under Indian law". However,

the government can issue a statutory license over it if the person is not ready to share the data with anyone and claim access over it for benefit of the public as well, they clarified.

Pune Smart City Pilot Project: “In Pune, they have a catalogue of public data coming from tools like traffic lights, air pollution, sensors trash cans and so on,” a participant said. This is an open data set, but its accuracy is not guaranteed. But, it’s possible to see which entities created the data, where they acquired it from, frequency with which it has through an API, you can also access the data. “The processes of monitoring, generating, storing, and consuming data have evolved to a significant extent,” they said. **But the process of consuming data is not part of this exchange and it is an entirely offline process.**

Open data from utilities owned by the utilities: A person who runs an electricity data start-up said that their company acquired a lot of data from the utility. This data is not related to any individual, and the company cannot “trace it to a person or a community or a housing society”. As per this speaker, **this data would be owned by the utility**, and “since it is available to the public, it would qualify as an open data set, and we [the private company] have limited control over it”. However, monetising this data is dependent on the quality of data in terms of the granularity and whether it is available in real time. “If the data is two weeks old, it is less valuable than data which is real-time,” they explained. “There is really no way a utility can enforce any right or any claim over ownership unless they say that we are not going to provide you granular data or real time data, which might be more valuable than old data or something like that,” they said.

Power industry and data sharing: There is a lot of data sharing that occurs in the power industry in Europe and North America, a participant shared. This is because “the data is used to enable better functioning of markets as electricity has a time-of-day pricing”. India does not have that concept, but has power trading. “This is why the processes of data collection, sharing and consumption in order to monetise have improved,” they said. They also clarified that some data is shared by choice, but some data is shared on a mandatory basis to enable power trading. These decisions are made by the Central Electricity Authority.

‘Government is using privacy as an excuse to stifle transparency’: When it comes to government access to data, a speaker pointed out that transparency is very important. This was visible in the case of electoral bonds as well. “RTI activists use MIS data from NREGA, PDS and other schemes to track government welfare schemes, and to find out about any leakages, scams, etc.,” they said.

Sharing data with private entities

“Value of data increases when it is shared and when it is extrapolated against other data sets,” a speaker remarked. Financial data is one such data set. It is this kind of data sharing that needs to be regulated, according to the participant. It also raised a question of whether such data sharing would be voluntary or mandatory, and who would bear the liability for ensuring its accuracy.

Sharing data with competitors is possible in certain circumstances:

“Competition law says that when the competition has no hope of surviving in the market without that particular data or proprietary information, or the person who holds that data intends to create a monopoly, it is only in those circumstances that the data should be shared,” an advocate explained. Courts around the world have held to this. India, given its nascentcy in competition law, follows the European example. To prove grounds for data sharing, there’s a balancing act: the company/entity needs to show an objective justification of need and the IPR holder needs to show that they don’t intend to create a monopoly.

- A person associated with a start-up said that when it comes to data access and sharing, competitive concerns are important. “Can the person who has access to data protect their interests from a competing entity which also has access to the data or the entity, which is creating data?” they asked.
- Similarly, standard-essential patents (SEPs) on smartphones were hurdle a few years ago as it takes about 60,000 SEPs to make a smartphone.
- **But, this is not justified:** A person from a private company disagreed that data should be shared with the government or another entity. “I don’t think it’s justifiable to take data away from a cab aggregator to formulate better policy around public transportation. I don’t think it’s justifiable to take an e-commerce company’s data to enable a local rival. These are non-tariff barriers to entry and function,” they said.

Can *sui generis* databases be made accessible to the public, including competitors? A lawyer argued that certain categories of Indians could be given access to such databases for a fee. Taking the instance of the German Autobahn, which has a *sui generis* right over the toll data for people using the Autobahn, they said that researchers can access this data for a lower fee.

Compensation is necessary for granting access, they argued. They said that it is possible to mandate that certain *sui generis* databases be made accessible to the public, including potential competitors, for a fee, but it is not possible to mandate that databases that fall under copyright/trade secrets be made accessible to the public.

- When vaccines were compulsorily licensed to competitors, the argument was based on the principle that “if the cost of access is too high, there is too much friction, then you can license it out into a common pool,” they explained. Health data is made available to competitors in emergency

services.

Who bears the liability for publicly sharing data sets? A speaker responded by saying, “in the absence of regulatory certainty about how research data, or non-personal data, or community data can be treated, it makes no sense for large companies to incur the liability and potential harm that they will incur by putting the data out for good”.

Trade secret data is not a property right: A lawyer in the room clarified that in most jurisdictions, trade secrets’ data is not a property right unlike copyright, which is almost like a property right, but over intellectual property. Moreover, India does not have a law related to trade secrets. “But in relation to IP, you have limitations and exceptions for each type of property, such as fair use and fair dealing,” they said.

*

Read our coverage of the our discussion on Non-Personal Data in Delhi here. The discussion was held in New Delhi on November 28, 2019, with support from Amazon Web Services, Facebook and FTI Consulting.

#NAMA: Why does the Indian government want to regulate non-personal data?

When it comes to data, the primary aim of the government is to earn money, and “the only way they can earn is when they actually sell personal data in a non-personal way”, said a speaker at MediaNama’s roundtable discussion on non-personal data. Speculating about the intentions of the committee of experts that is working on non-personal data, especially Avanti Finance CTO Lalitesh Katragadda, a speaker said that the committee wants to “**ring fence the Indian data economy so that data that is useful for India’s national development can be used by Indians**”. They likened it to rise of similar debates in other parts of the world including Germany (“data sovereignty” and “community data”) and France. Another participant highlighted the few stated objectives of government when it comes to data governance: economic growth, its governance, and privacy protection.

(Note: The discussion was held under the Chatham House Rule; quotes have not been attributed to specific people. Quotes are not verbatim and have been edited for clarity and to preserve anonymity. Also note that this discussion took place before the PDP Bill, 2019, was made public.)

Why does the government want control over non-personal data?

- **Some private data is valuable to community:** Globally, there is now an understanding that some companies dominate the global data market. From that, a speaker highlighted, has emerged an idea that “some of this data is valuable to the community”. While how this community data is defined remains up for debate, “some data that private companies hold can be used for social good/purpose” was potentially the primary goal behind creating the committee of experts, they said.
- **Data trade:** Another speaker guessed that the committee wants to formulate a policy that allows data in certain market segments to be traded in the Indian marketplace. They suggested that the committee could follow the national AI marketplace model, but that is also rife with issues: intellectual property, ownership questions, pricing data sets given lack of economic studies around that, etc. “These are the kinds of discussions that are happening right now: how do you price the data sets, how do you ensure that it is tradable as a commodity, is it tradable as a commodity, if it could be a marketplace, if it would have the ordinary rules of a securities’ marketplace, etc.,” they said.
- **Regulating group behaviour:** A participant pointed out that the government’s policies and general statements, both at national and international fora, about data colonialism and data sovereignty show that the “government is interested in collecting certain forms of data for economic and political purposes of regulating group behaviour and knowing more

about the Indian population”. According to the speaker, that is already happening, as proven by “legal mandates such as localisation”.

What kind of data does the government seek to control through non-personal data governance?

- **Data from IoT devices:** Remarking that the “government wants to create a governance framework(s) for all data”, a speaker said that the government wants “personally sourced data which is not sourced from personally identifying information”, and thus means data from sensors and IoT devices. Thus, according to the speaker, “a lot of the argument is about how such data has to be governed, regulated and perhaps shared with and used by start-ups”.
- **Behavioural data:** A participant pointed out that the government is looking at behavioural data which can include personal data. “This can be, in their [government’s] mind what might be anonymised or well-anonymised data, but it is also data about communities and groups and how to model behaviour using data,” they said. They highlighted the government’s concerns that data-based behavioural models are currently created and implemented by large technology companies that are based outside of India. “There is a very large economic rationale for why they want to regulate and localise this kind of data, and ensure more control over the kind of behavioural models that are created,” they said. The speaker cautioned against using data modelling to regulate human behaviour and the need to limit access to it, and its use: “The whole identity crisis that the Open Data Movement had was because they did all the groundwork to create an open maps infrastructure, which was ultimately misused by builders to demolish slums.”
- **Consumer spend and health data:** A speaker pointed out that in a 2014 paper, iSPIRT, a Bangalore-based lobby of technology companies in India, had said that consumer spend data belonged to the community. In a 2019 paper, they said that about health data. As a result, the committee on non-personal data would also want to regulate consumer spend data. “Consumer spend data is found in e-commerce, it is found in the financial sector, it is found in the non-banking financial sector. Incidentally, these are also sectors where you will see increasing technical mandates,” the speaker highlighted.

Factors to consider while governing non-personal data

A participant speculated that the committee on non-personal data would probably propose a policy that “incentivises return of certain kinds of data sets to a marketplace of sorts”.

- **Use must govern policy:** A number of participants agreed that the governance of non-personal data should be governed by how the data

is used. That should include establishing how the data would/should be used, who its owner is, what kind of risks it poses to users and establishing thresholds for it, etc.

- **Ownership of data determines policy:** As consent over NPD is considered, it boils down to who owns the data, a participant said. “When ownership comes into play, IP comes into play, as do anti-trust and competition issues. There has to be some sort of regulation now who should regulate these considering these are the issues that come out of use of NPD data and ownership,” they said.
 - For a lot of corporates, data is a business asset. A speaker used the example of a truck driver to illustrate their point: “If I am a truck driver who always comes to the mining operation drunk, my actions are behavioural data. Is it corporate data? Does it belong to me? Should it be used punitively against me? Should it be used to prevent other people from coming to work drunk? Should it be used to look out for signs in other people?” They also highlighted how if this data is traced back, it could be used to persecute people.

However, a lawyer said that “**it is not about who owns the property, but what uses are made of that property which should determine how it is regulated**”, with respect to data collected by instrumentation in smart cities. They clarified that even though the basic principle of jurisprudence, governed by John Locke’s theory of labour, says that “anybody who puts effort into collecting certain information or collecting certain data becomes the owner”, in this case, it should be regulated by use.

Benefits of processing non-personal data

- **Certain level of granularity can help in emergencies:** In certain situations, more personally identifiable data is more useful, a person said. Taking the example of a flood, they said, if a government passes a law that says they need location information at an aggregated level for the lake for the last 24 hours. “We will store it in a particular manner, and once the situation is sorted, will delete the information. In emergency situations, certain kinds of location data, if governed well, is of immense use to society. And if that data is deleted immediately after that and not used for anything else, it is a positive net gain,” they said.
- **Track spread of diseases:** Another person said that if the government wants to map out spread of disease, it would be useful to see in which direction it spreads, so that it can take steps to mitigate and halt the spread.

Harms of processing non-personal data

- **Biased, inaccurate data collection can lead to ‘horrific’ outcomes:** If the aim is to create a kind of public commons of non-personal data, we

need to be especially careful about the kind of inherent biases that may be built into databases, a participant warned. Cautioning that use of AI and ML would mean that a human might not even look at some of these decisions, they said that “if these data sets are not properly curated, if the data that is fed into these data bases is not accurate, significant decisions could be taken about entire populations and communities with inaccurate and biased data”.

- **Non-personal data, combined with other data sets can be used to target (groups of) people:** Taking the instance of a popular browser, a speaker highlighted how it collects an “astonishing amount of telemetry data”. A lot of this data, which is not associated with a personal identifier and the related IP address is not “regarded”, is publicly available on GitHub as open data set for people to work with.
 - This data includes: how long people take to connect to the website, the websites themselves, which websites are working, how long an application is open, etc. If this non-personal data is combined with other data sets, it could be used to block the internet in particular regions or decide which websites are popular or not. Another speaker said that when fintech data “comes together”, “it is quite beautiful from a marketing perspective, but from an individual’s perspective, it can be extremely dangerous”.
- **Misuse by government through sale and merging of data sets:** Taking the example of the government selling vehicular data to private companies, a participant said how the Bulk Data Sharing Policy allows that. As a result of this policy, if there is any misuse of personal identifying information, violators can only be looked at under the Information Technology Act, but data protection itself is not a tenet of it. Another speaker drew attention to the fact that the Bulk Data Sharing Policy “actively discourages merging different data sets” and the onus of misusing such data would be on the companies who buy it.
 - The previous speaker also brought up a new committee formed under the Insurance Regulatory and Development Authority of India (IRDAI) that is looking at whether traffic violations can be linked to motor insurance premium. The committee, they said, is headed by a person from HDFC bank and consists of many private and public insurance companies along with officials from the Delhi Police.
- **Sale of aggregated data:** A speaker commented on how a lot of aggregated data is sold by PR companies. The trends that then emerge are used to profile and specifically target specific people for a whole host of purposes.
- **Group privacy remains ignored:** A speaker cited the Sidewalk Labs project in Toronto to highlight how community data can be used for behaviour modelling and to profile communities. “Google’s open infrastructure and technology arm, Sidewalk Labs, entered into a public-private partnership with a neighbourhood in Toronto. Under this project, Google embedded passive sensors within urban infrastructure to decide how streets

and traffic management is going to happen, what kind of neighbourhoods get developed, how do you locate the most essential communities to allocate resources to and so on,” they explained. While this may not look at individual data, but data is being processed to formulate public policy, group privacy is not considered and such schemes allow for greater state surveillance as well.

What can be done to prevent some of these harms?

A lot of the harms associated with non-personal data are also possible with PII, a speaker said. To that end, they suggested some ‘Lean Data Practices’ that can be implemented to mitigate these risks. These include norms around data collection, data storage, data processing, and deletion of useless data.

Not share certain personally identifiable information (PII) with government: A speaker suggested that we could come up with a list of PII that should never be present in data sets that are shared with the government.

How will consent work?

A speaker pointed out that thus far, consent has not been taken into account when considering anonymised data. Another participant said that as we consider consent, it all boils down to who owns the data.

- **Consent doesn’t come into the picture:** Since data is irreversibly anonymised by the data processor, it becomes the IP of the processor, and thus the question of consent does not really arise, argued one speaker.
- **Without consent, there can be other harms:** Taking the instance of demographic information, a person asked if they could refuse to consent to it. “I don’t want things like my religion being used even in an aggregated way because aggregated anonymised non-personal data, which was originally PII, can lead to significant harms,” they said. They took examples of databases in Andhra Pradesh and Telangana that can be analysed for religion and yield gram panchayat-wise percentage of Hindus, Muslims, etc.

*

Read our coverage of the our discussion on Non-Personal Data in Delhi here. The discussion was held in New Delhi on November 28, 2019, with support from Amazon Web Services, Facebook and FTI Consulting.

#NAMA: Recommendations for governing non-personal data; what data trusts are

The government should draw inspiration from the Personal Data Protection Bill, 2018, to oversee government access to non-personal data, and there must be a system of checks and balances, a speaker said at MediaNama's roundtable discussion on non-personal data, held in November 2019. A number of recommendations for governing non-personal data emerged. Most participants agreed that any framework that the government or the committee of experts on non-personal data came up with should keep the following questions in mind:

- What is the due process of law?
- Who orders access to non-personal data? Is it responsible enough?
- What are the checks and balances in place for this access?
- Does it pass the test of public good?
- Where should those checks and balances be in place across the industry?
- When can the government make a trade-off between group privacy/autonomy and social good? Proportionality analysis of harms is necessary to answer this question.

Under this framework, a speaker clarified, the government should actually notify what data sets come under public good, national security, etc., and if they pass those tests. However, a participant disagreed and said that we don't need separate regulation for non-personal data and instead called for a more general protection against misuse of *all* data.

(Note: The discussion was held under the Chatham House Rule; quotes have not been attributed to specific people. Quotes are not verbatim and have been edited for clarity and to preserve anonymity. Also note that this discussion took place before the PDP Bill, 2019, was made public.)

Recommendations on governance

Public interest as a test, but share data with rivals on a case-by-case basis: A speaker said that when the government wants data for public policy, public interest is the obvious test. But for sharing data with competitors, it should be adjudged on a case-by-case basis; the government cannot decide that, it can only decide in terms of public interest.

Consider economic costs of sharing data with rivals: "If companies are chilled by the idea that the data sets they create are now going to be shared with their competitors, there may be an economic cost there that it's not going to be accounted for," said a speaker. The aim is to encourage, not stifle, innovation.

Targeted requests for data sharing to be handled by third-party: A participant suggested that targeted requests for data sharing should be handled by a third party. Also, there have to be clear rules about (mis)use and liability. Completely anonymised data can be put on MeitY's Open Government Data

Platform, and so can data that a private company volunteers to share with everybody.

Database rights are the way forward in the private use context: “Compelling access to a database protected under copyright would be akin to nationalising the data set,” argued a participant. And if that is what we are considering, we need to answer questions such as: what sort of eminent domain principle works over here? What are the guard rails? How do you compensate?

Have industry-specific data regulator: Another speaker recommended that data be a part of a regulator for every industry since the “standard of data sharing is very domain-specific”. For instance, an insurance regulator should have a department which specialises in data affairs, including its sharing, exchange, publicly available data sets, etc. One speaker said that the Data Protection Authority, proposed in the Personal Data Protection Bill, 2018 (and later in 2019), should not regulate NPD as it has too many things to sort out. Another speaker, agreeing with them, said, “With over 625 million internet connections, more than 500 million internet users, we will need a few DPAs to deal with the kind of issues we have in privacy itself.”

The concept of Data Stewards/Trusts/Exchanges

“The data steward sort of sits between the users and entities as well as people who are acquiring the data,” a participant explained. A data steward/trust:

- Has a responsibility or duty of care towards the users whose data it is.
- Potentially look at data as labour.
- Helps you negotiate better with technology companies.
- Looks at what the data is being used for.

Data trusts, according to the speaker, could be used to help share data between users and between entities. They could also answer questions such as how do we think about technology standards, quality of data, etc. Another speaker compared it to a regulatory sandbox. A different speaker called it a “good theoretical/conceptual framework to think about federated data governance for non-personal data”.

*

Read our coverage of the our discussion on Non-Personal Data in Delhi here. The discussion was held in New Delhi on November 28, 2019, with support from Amazon Web Services, Facebook and FTI Consulting.

Our initial comments on the Personal Data Protection Bill, 2019

In this blog post, we share our initial comments on the Personal Data Protection Bill 2019 (the Bill) that was introduced in the Lok Sabha in December 2019. Our preliminary research underscores seven key concerns that must be addressed to strengthen the proposed Bill and safeguard individuals' interests in the digital economy. These seven concerns are summarised below. A detailed 20-page document setting out research and reasoning to support these concerns, together with solutions to overcome them is available here. We welcome your feedback, challenge and comments on these initial comments.

1. User protections must be strengthened for the Bill to genuinely guarantee data privacy for Indians: We identify 7 consumer protection concerns that could weaken the citizens' right to privacy. Some are new concerns emerging in this draft of the Bill and some continue to prevail from the previous draft of the Personal Data Protection Bill released in 2018.

1.1 The Bill should not remove obligations to give notice to users where their personal data is processed without consent. The Bill dispenses with the data fiduciary's obligation to provide notice to data principals while processing personal data without their consent. Although non-consensual grounds of processing have always existed in the Bill, previously notice was required to be provided to data principals of such use in most of these circumstances except grave emergencies. The provisions in the current Bill are wider, increasing opacity for users when there is non-consensual processing of personal data. The Bill should still require notice in these circumstances.

1.2 The Bill should not raise high barriers for the data principals to withdraw their consent. The Bill makes the data principal liable for all legal consequences of withdrawing consent to process personal data unless they have a "valid reason". It is unclear why individuals should bear the threat of **all** legal consequences for withdrawal. This could disincentivise data principals from withdrawing consent. The Bill should not disincentivise data principals from withdrawing consent. Instead, withdrawal should simply result in termination of contract and discontinuation of related services.

1.3 The Bill should widen the suite of rights available to users' rights, to meaningfully empower them. The Bill contains a very limited set of rights for data principals. The absence of a full suite of user rights could result in the scales being tipped against users who may seek to achieve more autonomy and control over their data. Additional rights that can be included to level the field between data fiduciaries and data principals include: (i) right to clear, plain and understandable notice for data collection (ii) right to be asked for consent prior to data collection (iii) right to adequate data security (iv) rights to privacy by design (including privacy by default) (v) right to breach notification (vi) right relating to automated decision-making (vii) right to informational privacy (viii)

right against harm.

1.4 Data principals should not be charged fees (or be charged nominally) for exercising their rights. Data principals can be asked to pay a fee for exercising some of the rights in the Bill for e.g. the right to obtain a summary of the processing activity undertaken on their data, the right to data portability. We worry that charging a fee can raise barriers to exercise rights for low-income Indians who are becoming more digitally active but whose incomes remain low.

1.5 The Bill should not restrict users' right to seek remedies. Provisions in the Bill could limit individuals' rights to directly seek remedies in courts (where an offence is committed against them) or the Adjudicating Authority of the DPA (to initiate civil inquiries). The Bill states that a court or an Adjudicating Authority can only act upon a complaint filed by the DPA. Similar provisions restricting citizens' abilities to approach courts were held to be violative of rights by the Supreme Court when adjudging the constitutionality of the Aadhaar Act. Accordingly, these provisions (s. 83 and the proviso 63(1)) should be removed or amended.

1.6 The Bill should not make the notification of personal data breaches contingent on the breached entities' determination of "harm". The Bill requires data fiduciaries to issue a breach notification to the DPA only when they are satisfied that the breach is likely to cause harm. The DPA then determines if a breach notification should be conveyed to a data principal. Given that the concept of harm is not clear in the Bill (see point 5 below) it should not be the basis for deciding if breach notifications need to be issued. In addition, it requires that the breached entity itself that must make this determination. This could create the wrong incentives for companies suffering breaches, who now have to make a subjective decision of **whether** to report the breach. The process also creates a bottleneck at the DPA, which may delay notification of a breach to data principals. Instead, all data breaches should be reported to the DPA and data fiduciaries should have the freedom to reach out to data principals where direct actions are required following a breach.

1.7 The Bill should not weaken obligations for data fiduciaries to incorporate Privacy by Design, as this will reduce incentives to implement them. The Bill requires data fiduciaries to merely *create* privacy-by-design (PbD) policies that comply with its provisions. This obligation is weaker than that in the previous Bill which required data fiduciaries to *implement* PbD policies that would ensure compliance with its provisions.

2. The Data Protection Authority (DPA) needs to be strengthened for the new regime to be effective: The design, powers and functions of the DPA have been considerably weakened in the Bill compared to the previous Bill.

2.1 The design and composition of the DPA should be changed to maintain its independence as a regulator. The composition and design

of the Selection Committee and the Management Board are important ingredients required to create an independent, accountable and impartial regulator. Unfortunately, changes in the Bill risk compromising the quality of the future institution. No independent Members from technical and legal backgrounds are required to be part of the Board. The Selection Committee curated to appoint the Chairperson and Members of the DPA now comprises *only* Central Government officials (as opposed to the Chief Justice and an independent expert, as was previously the case).

2.2 Some substantive powers of the DPA that have been removed should be reinstated. Certain powers of the DPA have been removed or re-allocated to Central Government (compared to the previous Bill). First, the power to notify categories of sensitive personal data has been shifted to the Central Government. It is advisable for the DPA to retain this power since it is closer to the market than the Central Government with a day-to-day understanding of data practices that will enable it to make such a decision in consultation with its regulatory peers. Second, the power to notify significant data fiduciaries is not exclusively with the DPA in the Bill. The Central Government has the power to notify *social media intermediaries* as significant data fiduciaries. The power to notify significant data fiduciaries should be retained with the DPA (though it can consult with Central Government) for consistency in the delegation of powers. Third, the DPA is no longer required to publish results of inspections and other comments in the public interest. This obligation should be retained to ensure transparency in regulation, which has been proved to benefit the regulator and strengthen the regulatory regime.

3. Immense powers and exemptions for the State will limit the effectiveness of the new regime: Section 35 of the Bill empowers the Central Government to pass orders to exempt itself or any of its agencies from any or all provisions of the proposed data protection regime. This provision is a dramatic shift from the exemption for the State provided in the earlier draft of the Bill (under the 2018 draft Bill's section 42 (*Security of the State*))). It affords wide powers to the Central Government abrogate the fundamental right to privacy through executive order, without clear guidance and safeguards to fetter and guide the Central Government's exercise of power.

Other approaches such as inclusion of judicial oversight mechanisms in the section, or specifically setting out clearer conditions for the exercise of a power or the use of are better alternatives to ensure legitimacy and proportionality of this provision, and ensure it is not adjudged to be arbitrary. For instance, section 42 of the previous version of the Bill required such restrictions to be by "*procedure established by such law, made by Parliament and is necessary for, and proportionate to, such interests being achieved*". If not, in its current form the wide powers delegated through section 35 without clear guidelines for its use of other safeguards could open the provision up to the constitutional challenge.

4. The Bill should strengthen consumer protections within the proposed sandbox participants, and clarify its objectives: The Bill envis-

ages a sandbox “*for innovation in artificial intelligence, machine-learning or any other emerging technology in public interest*”. However, we have serious concerns on the user protection afforded provisions in this provision. A data fiduciary that is accepted into the sandbox could be bound only by modified and diluted forms of user protection obligations in Chapter II of the Bill. Sandboxes perform experimental operations using personal data exposing users to new risks, and its effects may not be immediately understood. The Bill should clearly set out and strengthen the user protections for individuals that are common in sandbox frameworks around the world and in India (in the RBI’s sandbox). Further, the objectives of the sandbox are unclear which could result in overlaps with other sandbox efforts (such as the RBI Sandbox).

5. “Harm” should not be a condition on which rights and obligations depend in the Bill: The Bill makes harm a precondition for twenty-three provisions in the Bill relating to user protection, fulfilment of provider obligations and enforcement by the DPA. This is worrying because the definition of harm in the Bill is unclear, resulting in it becoming a subjective assessment by entities, severely weakening all provisions that are predicated on the occurrence of “harm”. Rights and obligations in the Bill should be fulfilled irrespective of the occurrence of harm.

6. The Bill should not include provisions relating to the sharing of Non-Personal Data: The Bill includes three new provisions relating to use of anonymised and non-personal data by the Central Government. These provisions are not related to the objectives of the Bill (i.e. personal data protection) and should not be included in the Bill. Policy on non-personal data should be dealt with separately, and by the separate Committee set up by the Government in September 2019 to study various issues relating to non-personal data.

7. The Bill should contain transitional provisions to create certainty about its implementation: The previous Bill provided transitional provisions that clearly laid down the timelines within which its provisions had to take effect, including the establishment of the DPA. Clear timelines help create political will and industry preparedness to implement the data protection regime. There are no comparable provisions in the present Bill, which can severely impede its implementation and data fiduciary compliance. The absence of a timeline to give effect to the regulatory regime for personal data processing can ultimately set back the constitutional guarantee of the fundamental right to privacy.

The detailed document containing these initial comments is accessible here. We welcome your comments and suggestions to engage further on any of these issues.

SAVE OUR PRIVACY

A public brief and analysis on the **Personal Data Protection Bill, 2019**

IFF's briefs focuses research to support public understanding on issues of digital rights

Further analysis and guides available at : saveourprivacy.in

#SaveOurPrivacy

The #SaveOurPrivacy campaign has close to 11,000 individual and 27 organisational supporters who have pledged support to its 7 privacy principles and a model law titled as the, "Indian Privacy Code". The Indian Privacy Code has been filed twice as private members bills in Parliament.

#SaveOurPrivacy has worked since May, 2018 as a framework for civil society groups to put forward demands on data protection and surveillance reform. It has influenced and brought accountability to the drafting process of the Personal Data Protection Bill.

This brief has been authored by SaveOurPrivacy volunteers (Maansi Verma, Vrinda Bhandari, Gautam Bhatia, S. Prasanna, Raman Chima, Anushka Jain, Apurva Singh, Shreya Tiwari, Ishika Garg and Apar Gupta,) to assist legislative engagement.

#SavingTheInternet

The Internet Freedom Foundation works on issues of online censorship, advocating for privacy, safeguarding net neutrality and innovation.

It is a registered 80G non-profit funded by Indians and represents the interests of individual Indians.

We are guided by values of human freedom from the Constitution of India. Born out of the #SaveTheInternet.in campaign for Net Neutrality, IFF today supports research, advocates civic education, builds participatory campaigns, engages with regulators and approaches courts.

IFF powers the community driven #SaveOurPrivacy campaign.

For SaveOurPrivacy: www.saveourprivacy.in

For IFF: www.internetfreedom.in

6 Key facts on legislative history

- Present status:** The Personal Data Protection Bill, 2019 was introduced in the Lok Sabha by Union Minister of Electronics and Information Technology, Mr. Ravi Shankar Prasad, on December 11, 2019. A Joint Parliamentary Committee was formed on December 12, 2019 to review the proposed Data Protection Bill which is expected to give its report by the last week of the budget session of 2020.¹
- Past efforts:** Previous versions of a Draft Privacy Bill have been coordinated through the Ministry of Personnel, Public Grievances and Pensions since 2011.² Drafts of this Bill dealt both with Data Protection and Surveillance Reform till 2014 - however this did not proceed further.³ An Expert Committee on Privacy headed by Justice A.P. Shah under the erstwhile Planning Commission presented a report on October 12, 2012 which serves as an influential document on international & national privacy standards.⁴
- Private Member Bills:** There have been six notable efforts to introduce various models of privacy protection by honourable members of the Lok and Rajya Sabha. These are listed in a tabular form below.

House and date	Short title (click to download)	Member	Status
Lok Sabha on 04/03/2011	Intelligence Services (Powers & Regulation) Bill, 2011	Manish Tewari	Lapsed
Rajya Sabha on 05/08/2016	Right to Privacy of Personal Data Bill, 2016	Vivek Gupta	Lapsed
Lok Sabha on 10/03/2017	Right to Privacy of Personal Data Bill, 2016	O.P. Yadav	Pending
Lok Sabha on 21/07/2017	Data (Privacy and Protection) Bill, 2017	Baijayant Panda	Lapsed
Lok Sabha on 03/08/2018	Data Privacy and Protection Bill, 2017	Shashi Tharoor	Lapsed
Lok Sabha on 26/07/2019	Personal Data and Information Privacy Code Bill, 2019	D. Ravikumar	Pending

- Right to Privacy Judgement:** On 24th August, 2017, the Supreme Court in the matter of *Justice KS Puttaswamy vs Union of India* reaffirmed "privacy" as a fundamental right under Part III of the Constitution of India. It directed the Government to bring out a robust data protection regime.⁵
- Srikrishna Expert Committee:** The Expert Committee on Data Protection chaired by Justice BN Srikrishna was constituted by the Ministry for Electronics and IT on 31st July, 2017.⁶ It was criticised for its flawed composition and issues of conflict of interest.⁷ The Committee released its Report and proposed the Personal Data Protection Bill, 2018 on 27th July, 2018.
- Consultation by MIETY:** The PDP Bill, 2018 was open for comments in a consultation organised by the Ministry for Electronics and IT till October 10, 2018. However the comments, changes made to it, reasons and who made them were not made public by the Ministry. These changes were forwarded to the Union Cabinet and thereafter introduced in the Lok Sabha as the PDP Bill, 2019.⁸

¹ <https://prsindia.org/billtrack/personal-data-protection-bill-2019>

² <https://pib.gov.in/newsite/erelcontent.aspx?relid=74743>

³ <https://cis-india.org/internet-governance/blog/report-of-group-of-experts-on-privacy-vs-leaked-2014-privacy-bill>

⁴ <https://iltb.net/summary-of-the-report-on-privacy-law-by-the-group-of-experts-headed-by-justice-a-p-shah-6e5917ea9c18>

⁵ <https://indiankanoon.org/doc/91938676/>

⁶ <https://pib.gov.in/newsite/PrintRelease.aspx?relid=169420>

⁷ <https://indianexpress.com/article/india/citizens-group-questions-data-privacy-panel-composition-aadhaar-4924220/>

⁸ <https://saveourprivacy.in/blog/the-purpose-of-public-in-public-consultation-lest-we-merely-consult>

Summary of top 10 issues

Loopholes in the PDP Bill, 2019

1. Lack of clarity on the objectives : From the time of the Justice Srikrishna Committee, the PDP Bill has suffered a lack of clear focus on data protection. Instead it has incorrectly sought to promote private and state interests. This has resulted in confused drafting choices.

2. Preference to private and fiscal interests over data protection: The PDP Bill, 2019 creates large carve-outs for anonymised non-personal data, sandboxes that would undermine the privacy rights of individuals on grounds of lack of consent. There peculiar insertions not found in global data protection laws.

3. Collection of data without consent and denial of services: There exist broad conditions which can make the government and other entities collect data without consent and also deny essential services.

4. Strengthen user rights: While several user rights are present, rights such as being exempt from automated decision making are not granted to people. Further exemptions and carve-outs need to be re-examined.

5. Social Media Entities: The provisions with regard to social media entities using government ID's for verification is completely misplaced. It would have several harms, increase surveillance and profiling.

6. Data localisation: The data localisation provisions are improperly placed within the data protection law. They are broad, vague and provide tremendous discretion to the government.

7. Surveillance reforms: One of the most obvious deficiencies of the PDP Bill, 2019 are the large exemptions provided to Government by which it can exempt its own departments from application of the law. Further, there is a complete absence on seizing the historic opportunity for surveillance reforms.

8. DPA's selection, staffing and independence: Another core deficiency in the PDP Bill, 2019 is the lack of independence of the DPA's selection body which comprises only of government officials without having any judicial, opposition or civil society membership. This becomes important given that the DPA is institutionally meant to protect individuals both against private and government entities.

9. Miscellaneous: Provisions on impact to the RTI Act and the need for application of the protections to only natural persons must be considered.

10. Protection for vulnerability testers and whistleblowers: The exemptions within the PDP Bill need to spell out clear protections for those who protect and further cyber security by vulnerability testing and reporting on breaches.

Analysis

Concern and clauses	Analysis	Recommendations
I. Lack of clarity on the objectives Preamble	<p>The preamble of any law sets the tone and the tenor of a law and is crucial in understanding the intent behind the legislation. The preamble, along with the objects, is also a key factor influencing the judicial interpretation of various provisions of the law.</p> <p>The preamble of the PDP Bill, 2019 contains objectives on creating a collective culture which promotes a free and fair digital economy, progress and innovation, while respecting informational privacy. Such emphasis on promoting digital economy through a data protection legislation - rather than prioritising the rights of Indians - is misplaced. There seems to be a tangential focus on economisation of data as opposed to a clear and unequivocal emphasis on the individual privacy as a fundamental right.</p> <p>The preamble also makes no mention of safeguarding a citizen's right to privacy from the state. The history of the evolution of the right to privacy, both globally and in India (especially as happened by the Aadhaar litigation), demonstrates a recognition of the need to protect privacy against State action. A modern data protection legislation must not only embody this recognition, but go further and exhort the State to be a model data controller.</p>	<p>The preamble be suitably amended to state, in no uncertain terms, that protection of data and informational privacy, from private as well as state actors, is the overriding objective of the PDP Bill. Once a data protection law and its modalities are in place, suitable compliant norms can then be designed for other related concerns.</p> <p>The preamble must also be suitably amended to state the principle of the State needing to be a model data controller. Here, we must refer to the individual rights of natural persons in line with the Supreme Court's right to privacy judgement and the model privacy principles recommended by the A.P. Shah Expert Committee Report</p>
2. Preference to private sector and financial interests over data protection Clauses 2(B); 3(2); 3(3); 40; 91.	<p>Provisions of the PDP Bill will not apply to anonymised data (Clause 2(B)). Anonymised data is such which has gone through an irreversible process of transforming or converting data to a form in which the data principal cannot be identified as per standards of irreversibility specified by the Authority (Clause 3(2) and 3(3)). However, in consultation with the Authority, the Central Government can mandate any data fiduciary or processor to provide it with anonymised personal data or other non-personal data (defined as data other than personal data) for better targeting of services and "evidence based policy making". The Central government may also frame policies for the digital economy as long as it does not govern personal data (Clause 91).</p> <p>There is no clarity on what is non-personal data. The definition of anonymised data is not comprehensive and leaves out the possibility of identification of data principal by combining anonymised data with other data - which is increasingly possible today. Additionally, the Bill provides for setting up of a 'Sandbox' to privacy regulation, without even defining the term anywhere (Clause 40).</p>	<p>A data protection legislation must not have an enabling provision for the government to mandate sharing of non-personal and anonymised data with it, for setting up regulatory 'sandboxes' and for framing policies on digital economy, especially when the possibility of misuse of anonymised and non-personal data and threats arising from new technology have not been sufficiently addressed. Real possibilities exist of identification and subsequent targeting of individuals and communities from seemingly non-personal data. These provisions are not usually present in Data Protection Acts globally and are a deviance from the objective of the present legislative proposal. We recommend their deletion.</p>

Concern and clauses	Analysis	Recommendations
<p>3.</p> <p>Collection of data without consent and denial of services</p> <p>Clauses 11; 12; 13; 14; 16.</p>	<p>Clause 12 lays the grounds under which personal data may be processed by the State without consent of the data principal, including for providing services, benefits, licenses, compliance with judgment or order of the courts, to respond to medical emergencies, undertake measures during disaster or any breakdown of public order. Additionally, the exemption from consent also applies to personal data collected by employer for recruitment, verifying attendance, performance assessment etc.(Clause 13) and even to other 'reasonable purposes' (to be identified through regulation) which can range from whistle-blowing to operation of search engines (Clause 14).These exemptions are broad, vague and pose concerns on excessive delegation and undermine the right to privacy. It further requires consent on behalf of minors to be given by a guardian and a responsibility is put on data fiduciary to verify the age of data principal (Clause 16).</p> <p>It is provided that the provision of a good or service or enjoyment of a legal right or claim etc. shall not be denied for want of consent to process data not necessary to that purpose. However if consent given is later withdrawn, without any valid reason, the data principal will be liable for all legal consequences (Clause 11). There is no express bar on denial of essential services and it is not clear whether such legal consequences will amount to denial of essential services.This is important to note because there have been many instances where essential services like rations, medical aid have been denied to beneficiaries.</p>	<p>It is imperative that the Bill provide an explicit bar on denial of essential services for want of personal data or at the very least be based on the impossibility of providing the service. It must mandate for a data fiduciary to provide for and accept less intrusive alternatives to particular personal data. It is also important that any collection of data without consent is strictly for a limited purpose and the law shouldn't provide any scope for further addition to this through delegated legislation.</p> <p>A child should be able to rescind consent upon attaining majority; other people who may be incapable of giving consent should be covered.</p> <p>Regarding use of data by employer without consent reference may be made to Article 88 of European Union's General Data Protection Regulation, which provides for processing of employee's personal data in context of employment while safeguarding human dignity, legitimate interests and fundamental rights - especially with respect to transparency of processing.</p>
<p>4.</p> <p>Strengthen user rights</p> <p>Clauses 18; 19; 21; 25.</p>	<p>Clause 18 contains the right to correction, completion, updation and erasure of data but are limited as the data fiduciary's obligation to respond to these rights has been made conditional and it may even refuse a user request.</p> <p>Clause 19 contains the right to data portability but again, data fiduciary may deny on grounds of technical infeasibility or protection of a trade secret. Here, personal data is not a trade secret as it primarily concerns the fundamental rights of persons.</p> <p>Clause 21 provides that for complying with requests made by data principles in exercise of their rights, data fiduciary may charge a fee.These rights are fundamental to a data principal, and she should not be charged for their exercise beyond a nominal fee.</p> <p>Clause 25 provides that in case of a breach of data, data fiduciary shall inform the Data Protection Authority, as soon as possible, where such breach is likely to cause harm to any data principal.</p>	<p>Clauses 18, 19, 21 and 25 need to be reviewed in an analysis in which the individual right to privacy receives primacy and the interests of data fiduciaries are limited exceptions, if any. Specifically, Clause 25 that empowers the DPA to determine whether to keep the data principal in dark in case of a breach of their personal data requires change to make disclosure of the data breach a rule.</p> <p>As far as possible, any unnecessary or unreasonable restrictions should not be placed on the exercise of rights. Further rights such as the right to seek exemption from automated decision making, especially when it can lead to violation of rights require inclusion.</p>

Concern and clauses	Analysis	Recommendations
<p>5.</p> <p>Social Media 'Registration' and Data Retention</p> <p>Clause 26</p>	<p>A social media intermediary has been defined in the Bill and it is provided that it can be categorised as significant data fiduciary depending on number of users and impact on electoral democracy, security of state, public order etc (Clause 26). Such social media intermediaries will have to enable their users to verify their accounts "voluntarily" in such manner as may be specified, and such verified accounts may be identified with some visible mark. It will adversely affect whistleblowers, victims of sexual assaults who often resort to anonymous identities on social media websites to share their experiences.</p> <p>It is not clear if the means devised are suitable to address the identified purpose. It will lead to further data collection by large social media companies on the basis of Government IDs and to the contrary facilitate more targeting and surveillance. Such a provision is not found in any data protection law globally and is a deviation from established privacy norms. This provision will also increase the risk from data breaches and entrench power in the hands of large players on the internet who can afford to build and maintain such verification systems.</p> <p>There are concerns that intermediaries through changes in the Information Technology Act, 2000 and its rules will have to report accounts that do not verify themselves to the government, which could make them a target for political censorship and chill dissent.</p>	<p>The vagueness and over-breadth of Clause 26 makes its constitutionality suspect. This provision must be removed and any regulation of social media intermediaries other than data protection must be through specifically tailored laws that Parliament carefully reviews and are careful about respecting fundamental rights.</p> <p>Concerns on social media companies (other than personal data) need to be considered separately under legal frameworks of electoral, intermediary liability, and competition laws.</p>
<p>6.</p> <p>Local data storage</p> <p>Clauses 33; 34</p>	<p>While there is no requirement for localisation for "personal data", the Bill however does state that "sensitive personal data" may be transferred outside India (by asking for explicit consent from data principal and taking additional safeguards including determination of whether adequate protection will be offered), but shall continue to be stored in India. "Critical personal data" is not defined in the Bill, Further the government is empowered to define critical personal data at a later stage, which may not be transferred outside India at all except for prompt action during a health emergency or to a country, entity or international organisation to whom Central Government deems permissible to transfer (Clauses 33 and 34). This provides the government with powers to collect and process data and when the Bill additionally mandates storing and processing sensitive and critical personal data in India, it is likely to create concerns of unbridled intrusion into privacy by the state. In the EU's GDPR, there are two categories of data- personal data and special categories of data. The former is similar to the definition of personal data in the Bill. The latter includes data pertaining to race, ethnicity, political opinions, religious beliefs etc. It is important to note that data localisation requirement is absent in GDPR.</p>	<p>The Bill must not mandate storing or processing of data only in India. Free flow of data, with adequate safeguards to ensure that data protection rights apply to the data of Indians no matter where it may be transferred truly protects privacy in our internet age while also helping make India a valuable player in the globally networked trade regime. Critical Personal Data, if at all, must be defined in the Bill itself by Parliament. It can not be left to be defined by the executive without any guiding principles.</p>

Concern and clauses	Analysis	Recommendations
<p>7.</p> <p>Surveillance Reform</p> <p>Clauses 35; 36; 37</p>	<p>Clause 35 of the Bill empowers the Central Government to exempt by an order, 'any agency' of the government from all or any provisions of the data protection law if it is in the interest of the sovereignty and integrity of India, the security of the state, friendly relations, public order and to prevent incitement to the commission of an offence. The only safeguard is that the written order from the Central Government must specify the reasons for such exemptions, ignoring the requirements otherwise established in Indian and international law of meeting the test of being "necessary and proportionate". These exemptions will not just apply to data gathered by such agencies, but also with any data that is shared with such agencies by other data fiduciaries. It puts the power in the hands of the Central Government and specifically makes it the judge and adjudicator of its own cause. Clause 36 of the Bill also creates specific exemptions in certain cases, to which no safeguards will apply. Clause 37 which is supposed to empower the Central Government to exempt the processing of data of foreigners by data processors is also vaguely worded. Most intelligence agencies of India suffer from a lack of institutional oversight and there are no laws clearly defining their powers or limitations to those powers. Further, there is the lack of any serious review of telephone tapping and other communications interception powers in the Bill. This will make personal data of citizens open to mass surveillance and make the protection meaningless.</p>	<p>Existing exemptions are too vague and broad and must be narrowly tailored. A complete chapter on surveillance reform needs to be inserted in the present PDP Bill. Government agencies responsible for carrying out surveillance and interception as part of their law enforcement functions must be clearly identified, notified, and bound by the provisions of the Bill.</p> <p>A procedure must be put in place for such agencies to seek permission from a judicial authority - preferably by special benches or tribunals comprising of High Court judges. Additionally, an appropriate oversight and accountability structure should be created as part of Data Protection Authority by adding within it an office for surveillance reform and oversight. Judicial permission that may be granted for emergency surveillance and communications interception must be required to follow the necessity and proportionality principles. To administer such judicial orders, the Data Protection Authority may determine compliance and enforcement mechanisms.</p>
<p>8.</p> <p>DPA's selection and lack of independence</p> <p>Clauses 42; 62; 63; 86</p>	<p>As per Clause 42, the Selection Committee for appointing members of the Authority will comprise entirely of members of the executive. The Srikrishna Committee draft bill of 2018 had prescribed a diverse selection committee with executive, judicial, and external expertise. Given that this proposed law is also safeguarding user data from the government, there is a lack of impartiality because the government itself will exclusively bring in place the governing structure. This will make it much harder for the DPA to be an independent and effective regulator.</p> <p>The Bill further impedes the independence of the DPA by empowering the Central Government to issue binding directions to the DPA (Clause 86). It must also be noticed that for the anticipated number of data protection grievances that people may have, there is no decentralization of the DPA to establish state level authorities. This can lead to pendency in the long term. Lack of independence of the adjudication wing is also of concern, since Adjudicating Officers will be appointed by the DPA (Clause 62) and will only adjudicate enquiries initiated on complaints made by DPA (Clause 63).</p>	<p>The composition of the Selection Committee must comprise of a judicial authority, an executive authority and external members. The process for appointment of the DPA Chairperson and Members must be transparent with an open call for applications and proceedings of the Committee must be a matter of public record. There must be a bar on persons with vested political or business interests to be appointed to the DPA.</p> <p>State level DPAs must be set up by enabling State Governments to do so, in line with other state level regulators like State Information Commissions. Appointment of Adjudicating Officers should also be through a transparent process and by independent bodies designed to select judicial officers. Central government must not have any power to issue binding directions to the DPA.</p>

Concern and clauses	Analysis	Recommendations
<p>9. Miscellaneous Clause 96; Schedule</p>	<p>It is important to note that the Bill doesn't acknowledge a natural person as owner of their data. The Bill also doesn't deal with data collected prior to the Bill coming into force and has no transition provisions. Additionally the Bill has been given an overriding effect (Clause 96).</p> <p>The EU GDPR repealed the EU's pre-existing Directive 95/46/EC popularly known as the Data Protection Directive. Recital 171 of GDPR provided that processing already underway under the earlier Directive should be brought into conformity with GDPR within two years after which this Regulation enters into force. Where the processing consent is based on the Directive, it is not necessary for the data subject to give consent under GDPR again if the consent has been in line with GDPR.</p>	<p>The Bill must categorically acknowledge a natural person as owner of her data. The Bill must additionally provide that data collected prior to this law coming into force, if collected in a manner inconsistent to the law, must be destroyed if the consent is withdrawn. Finally, the Expert Committee Bill had sought to amend the Right to Information Act specifically, whereas the current Bill has an overriding clause, and both may ultimately lead to undermining the RTI Act by stifling transparency. The Bill must specifically state that provisions of RTI Act will have precedence over this law in case of inconsistency.</p>
<p>10. Protection of whistleblowers, digital security researchers, vulnerability testers Clauses 25; 38; Schedule</p>	<p>In several cases of breach of the obligations under the Act - particularly in relation to the breach of the limitation of purpose obligation, unauthorised sharing or a non-notification of a security event, the data principal is often in the dark and is not in a position to enforce her rights due to the asymmetry of information. At present Clause 25 only provides for a data fiduciary to report such breaches and lapses rather than whistleblowers. It is important therefore for the Bill to provide an institutionalised mechanism for personnel of the respective data fiduciary to safely, and freely without any fear of retaliation or retribution, report such breaches.</p> <p>While research is exempted from the obligations of Clause 38 there are no clear protections for skilled cyber security researchers who conduct vulnerability testing. Many such persons are put to harassment by vexatious legal claims and proceedings.</p>	<p>The Bill must make amendments to provide include clear provisions detailing the procedure for security researchers, vulnerability testers, data breach reporting and whistleblowers to the DPA with suitable amendments to Clause 25. This is in addition to the direct breach notifications we have recommended above.</p> <p>Further amendments must be made to Section 43 of the Information Technology Act, 2000 to prevent vexatious legal claims and proceedings against vulnerability testers and cyber security experts. We recommend that narrowly tailored good faith exceptions must be added by way of an amendment to the Schedule.</p>

Contact us!

Whether you are a Member of Parliament, a technologist who works with data or an ordinary person intrigued by privacy; we encourage you to reach out to us!

We offer regular briefings and deconstruct some rather complex and nuanced policy debates into helpful guides and encourage wider public participation.

Just email us on policy@internetfreedom.in



**INTERNET
FREEDOM
FOUNDATION**

Yesterday, the Government of India shared a near final draft of its data protection law with Members of Parliament, after more than a decade of engagement from industry and civil society. This is a significant milestone for a country with the second largest population on the internet and where privacy was declared a fundamental right by its Supreme Court back in 2017.

Like the previous version of the bill from July 2018 developed by the Justice Srikrishna Committee, this bill offers strong protections in regards to data processing by companies. Critically, this latest bill is a dramatic step backward in terms of the exceptions it grants for government processing and surveillance.

The original draft, which we called groundbreaking in many respects, contained some concerning issues: glaring exceptions for the government use of data, data localisation, an insufficiently independent data protection authority, and the absence of a right to deletion and objection to processing. While this new bill makes progress on some issues like data localisation, it also introduces new threats to privacy such as user verification for social media companies and forced transfers of non-personal data.

As the bill is introduced and reviewed in Parliament, attention and action is needed on several provisions. Here are some highlights:

- **Exceptions for Law Enforcement and other government use:** The biggest concern in the new draft is the bill's expansion of the broad exceptions that were present in the 2018 draft of the data protection bill for the government processing of data. Crucially, the requirement that government processing of data be "necessary and proportionate" has been cut. Furthermore, a provision was added granting the government complete discretion to exempt any entity or department from any part of the law. This leaves the current legal vacuum around India's surveillance and intelligence services intact, which is fundamentally incompatible with effective privacy protection.
- **Independence of the Data Protection Authority:** The new law further reduces the powers and independence of the data protection authority (DPA) by significantly weakening the commission that will appoint the Chairperson and members of the DPA. Where the 2018 draft said that they were to be appointed by a diverse committee with executive, judicial, and external expertise, the new law limits this committee to members of the executive. As with the last bill, Adjudicating Officers are also appointed by the government. Together, this will make it much harder for the DPA to be empowered and effective as the entire governing structure will be appointed exclusively by the government.
- **Social Media User Verification:** In a move that will be disastrous for the privacy and anonymity of internet users, the law contains a provision requiring companies to provide the option for users to voluntarily verify their identities. This would likely entail users sending photos of government issued IDs to the companies. There are also reports that intermediaries will have to report accounts that do not verify themselves using

such procedures to the government, which could make them a target for government scrutiny and investigation. This provision will incentivise the collection of sensitive personal data from government IDs that are submitted for this verification, which can then be used to profile and target users. This is not hypothetical conjecture – we have already seen phone numbers collected for security purposes being used for profiling. This provision will also increase the risk from data breaches and entrench power in the hands of large players in the social media space who can afford to build and maintain such verification systems. There is no evidence to prove that this measure will help fight misinformation (its motivating factor), and it ignores the benefits that anonymity can bring to the internet, such as whistleblowing and protection from stalkers.

- **Forced Transfer of Non-Personal Data:** The law also mandates that certain companies can be forced to transfer non-personal data to the government for public good and policy planning purposes. Not only can non-personal data constitute protected trade secrets and the insights derived from such data be protected by intellectual property law, but turning over this information to the government also raises significant privacy concerns. Information about sales location data from e-commerce platforms, for example, can be used to draw dangerous inferences and patterns regarding caste, religion, and sexuality. The law should continue to focus on the protection of personal data and leave the regulation of non-personal data to an independent law.
- **Ambiguity in Implementation:** The 2018 draft clearly laid out the timelines for the creation of the data protection authority, the accompanying subsidiary legislation, and the date in which the law would finally be enforceable. The new law removes all references to this timeline and merely mentions that the Central Government may notify the enforcement of the law at its complete discretion, creating ambiguity and uncertainty in the ecosystem.

On a positive note:

- **Data Localisation and Cross Border Transfers:** In a positive move compared to the 2018 draft, the law relaxes data localisation restrictions and applies them to only sensitive and critical personal data (i.e., personal data can be transferred without restriction). For sensitive data, the data can be processed outside the country and there are also reciprocity based exceptions that allow even critical and sensitive data to be processed outside the country. However, sensitive data must be stored in India, and it continues to be hard to see this as anything other than an effort to make surveillance easier.
- **Right to Erasure:** In a positive move, the new law includes an explicit right to erasure along with the right to correction, which gives data principles the right to demand that fiduciaries delete data which is no longer necessary for the purpose for which it was originally processed.
- **Strong obligations on companies and rights for individuals:** Over-

all, the bill retains the strong protections in regards to processing by companies that existed in the 2018 draft. In particular, there are strong provisions on consent, authorized basis for processing, purpose limitation, collection limitation, notice, data retention, data quality, data security safeguards, right to access, right to correction, data portability, and enhanced obligations for significant data fiduciaries.

Overall, while there are several strong provisions, significant concerns remain with the law and the Parliament will be critical in ensuring that Indians receive the data protection law they deserve. Mozilla will continue to engage with the Parliament, the Government of India, and other stakeholders over the coming months to help make this happen.

New data bill gives sweeping powers to govt

| | Published 13.12.19, 07:11 PM

The new Personal Data Protection Bill- 2019 represents a positive step towards finally realising a data protection and privacy law for all Indians. It introduces principles of collection limitation, data retention and purpose limitation, and strengthens the existing notice and consent framework. However, at the same time, the bill extensively broadens the exemptions granted to the government from these and other data protection obligations, giving rise to significant concerns for citizens' privacy. Let's focus on three such exemptions in this piece — Sections 35, 36 and 12.

First, let's look at Section 35 which gives the government wide powers to exempt itself from the protections guaranteed to citizens under the bill. For instance, this section empowers the central government to exempt "any" government agency from "all or any" provisions of the act with regard to processing of specified personal data. The government can also take such a step if it is satisfied that it is "necessary or expedient" to do so in the interest of sovereignty and integrity of India, the security of the state, friendly relations with foreign states and public order. In addition, the government can also be given an exemption on grounds of preventing incitement to commit any cognisable offence relating to the sovereignty and integrity of India, the security of the state, friendly relations with foreign states and public order. Section 35 marks a stark contrast from the previous version of the Personal Data Protection Bill- 2018 released by the Justice Srikrishna Committee, which only exempted the processing of data "in the interests of the security of the state".

The 2018 bill granted the exemption for the processing of personal data if the processing complied with four conditions – first, it was authorised pursuant to a law; second, it was in accordance with the procedure established by such law, made by Parliament; third, it was necessary for achieving such interests; and fourth, it was proportionate in its application. These requirements were introduced to comply with the Supreme Court judgment in the landmark Justice K.S. Puttaswamy versus Union of India (Right to Privacy) case. That unanimous ruling held that Indians have a constitutionally protected fundamental right to privacy. The judgment further held that any exemption from the application of the act should be narrowly tailored. Even then, the 2018 bill was criticised for being a near carte blanche given to the government.

However, the 2019 bill removes these safeguards entirely and replaces them with a mere requirement that the central government pass an order, recording its reasons in writing, subject to "such procedures, safeguards, and oversight mechanism to be followed by the agency, as may be prescribed." In this manner, the government has left the important task of oversight and accountability to regulations that will be notified by the Data Protection Authority directly — and hence, will not be debated in Parliament — and will likely not include judicial oversight.

Another departure from the 2018 bill lies in the Union's power to exclude the application of the entire 2019 bill. In the previous iteration of the legislation in 2018, the Justice Srikrishna Committee had imposed minimal safeguards in the exercise of the exemption by the State by first, imposing a duty on it to process the data in a "fair and reasonable", privacy-respecting manner. Second, the 2018 bill required security safeguards to be followed, including using methods such as de-identification and encryption, taking necessary steps to protect the integrity of the personal data, and taking necessary steps to prevent its misuse. Third, the 2018 bill did not exclude the provisions of the bill that related to civil and criminal offences and penalties or the provisions pertaining to the Data Protection Authority. Unfortunately, the 2019 Bill does not even impose these minimal safeguards on the state.

The 2019 bill, thus, vests enormous power with the central government. Section 35 can completely exclude the application of the 2019 bill, and in the process, infringe on the privacy of an individual, based on its own satisfaction of the fulfilment of certain pre-conditions. In view of this, the lack of any prescribed safeguards; the lack of independent (parliamentary/judicial) oversight mechanism; as well as the removal of the requirements of legality, necessity, and proportionality are deeply troubling and likely to be struck down as unconstitutional.

Now, let's turn to Section 36. This section also exempts certain provisions of the 2019 bill for, *inter alia*, the processing of personal data in the interests of "prevention, detection, investigation and prosecution of any offence or any other contravention of any law for the time being in force". It also departs from the corresponding provision in the 2018 bill by removing the requirements of legality, necessity, and proportionality.

Apart from this, Section 12 permits the processing of personal data without the consent of the data principal if such processing is necessary "for the performance of any function of the State authorised by law" for the provision of any service or benefit to the data principal from the state. This is a broadly worded exemption and seems to cover the use of the PDS (Public Distribution System) through Aadhaar. The requirement in the 2018 bill that sensitive personal data may be processed for the exercise of any function of the state only when it is "strictly necessary" has also surprisingly been done away with. Section 19(2) further restricts the right to data portability if the processing is necessary for "functions of the State".

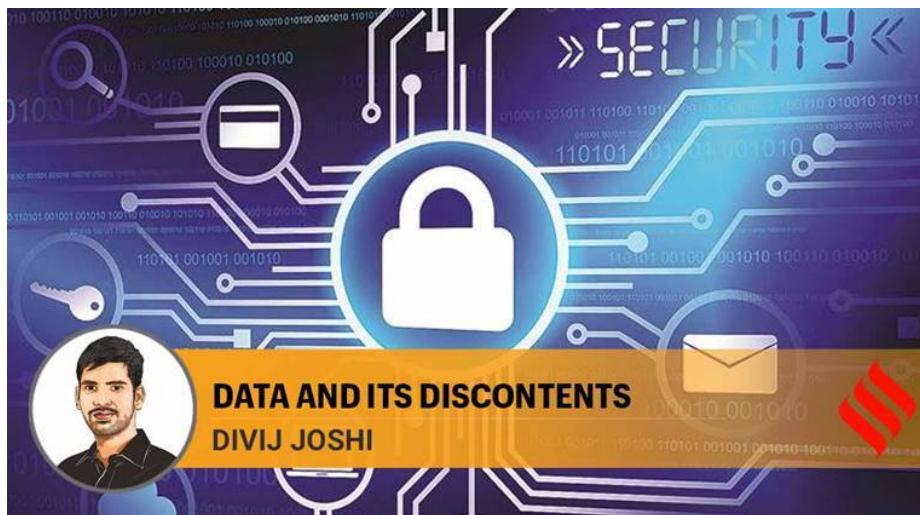
The underlying theme of this new data protection bill is to give even greater power to government. This manifests itself in various other provisions such as Section 91 permitting the central government from framing any policy for the "digital economy", insofar as such policy does not govern personal data.

The granting of increased power to the government, particularly the central government, must be accompanied by increased scrutiny. Now that the bill has been referred to the joint parliamentary committee instead of the parliamentary

standing committee on information technology, it is all the more important that the bill is properly debated and various stakeholders consulted. Only then can the true promise of privacy in the Puttaswamy case be retained and flourish.

The author is an advocate practicing in Delhi

Personal Data Protection Bill strikes a discordant note on ‘non-personal data’



“‘Anonymised data’ under the Bill refers to data from which markers of identity have been “irreversibly” removed,” writes Divij Joshi.

On December 11, 2019, the Personal Data Protection Bill was introduced in the Lok Sabha as a landmark legislation meant to safeguard the constitutional guarantees of privacy for Indian citizens and provide a just and equitable vision for the future of India’s digital economy. However, an incongruent provision in the Bill departs from this expectation — clause 91 enables the central government to direct any of the regulated entities under this Act to provide anonymised personal data or non-personal data to enable “targeted delivery of services” or “evidence-based policy making”. The implications of such a provision for India’s digital economy must be carefully considered as Parliament reviews the proposed legislation.

“Anonymised data” under the Bill refers to data from which markers of identity have been “irreversibly” removed. However, anonymisation should not be seen as a silver bullet for the use of large datasets without compromising privacy. Recent research shows that the common methods of anonymisation applied today are imperfect and data released as “anonymous” can be re-identified, particularly with the use of modern machine learning techniques. This renders large anonymised datasets vulnerable to “re-identification attacks”, where data from other sources can be combined to re-identify anonymised data and link it back to individuals.

OPINION by Udbhav Tiwari | Don’t rush into bad law: Giving India the data protection law it deserves

In the UK, personal location information has been extracted from anonymised

datasets of public transit, while in Australia, individual health records have been mined from anonymised medical bills. These examples should caution Parliament from allowing the government to acquire anonymised data without further protections — if anonymisation techniques are imperfect, then forcing companies to create and share insecure datasets with the government increases the vulnerability of personal information and undermines data protection. Going forward, the approach to regulation of anonymised data must be contextual and sectoral, targeting sensitive areas such as healthcare and finance, and focus on data aggregators, which are often used for reidentification attacks.

The proposal to acquire non-personal digital data must also be seen in the context of the Centre's push towards using "big data" and "artificial intelligence" technologies within governance and planning systems. Indeed, the use of these technologies has the potential to increase government capacity and transparency, as well as provide insight for making informed decisions about economic and social planning. However, the provision ignores the multiplicity of existing and inchoate rights and interests that exist within non-personal data, particularly those which are created by private firms.

OPINION by Akriti Gaur | Deconstructing the proposed draft data protection law

While the Bill assumes that any such data held by any entity should be open to acquisition by the government, similar to a power of "eminent domain" over land, this is in conflict with existing legal systems such as copyright law and trade secret protections. Such databases are commercially significant to private companies, and a law to acquire them must consider how it will affect their commercial exploitation. Moreover, the overlap of these existing rights within government systems can jeopardise accountability and transparency by limiting the ability of citizens to participate in, understand or interrogate government decisions. The RTI Act, for example, may not apply to private databases protected by intellectual property law.

The unregulated use of private datasets in governance also has consequences for the people and communities who are being made more visible, or are being invisibilised, through the use of this data. While the government has historically relied on qualitative methods like the census for understanding populations and their needs, the shift to quantitative methods and "big data" relies upon private datasets, which were created and used in a completely different context and for different purposes.

OPINION by M Sridhar Acharyulu | When it isn't right to forget

Inevitably, such data will be incomplete for the purpose of governance, and replete with the biases of the private entity creating and analysing the data. In the absence of regulation which carefully considers its limitations, using such data to target beneficiaries or for economic planning can have hazardous consequences — including arbitrary denial or exclusion from critical government services; or through biased and discriminatory planning which replicates biased data and

risks undermining important legal principles such as the right to equality before the law.

The regulation of non-personal data must take into account both the potential harms to individual privacy as well as the wider social and political consequences of such “datafication” of government. This is ostensibly why an expert committee was established to look specifically into the governance of non-personal data, even while the PDP Bill was expected to limit its scope to personal data of individuals. Instead of jeopardising both these goals and putting the cart before the horse, as the PDP Bill has done, the Gopalakrishnan committee must be allowed to deliberate and inform a public consensus on the appropriate models of governance of non-personal data.

The writer is a Mozilla Technology Policy Fellow

Power over privacy: New Personal Data Protection Bill fails to really protect the citizen's right to privacy

Earlier this year, in April, a data breach in the Election Commission of Philippines led to the leakage of personal information of over 55 million eligible voters on a searchable website: including names, addresses and date of birth. This was not the first data breach from the Election Commission. After the first, which took place in March 2016, where 340 GB of voter data was published online by a group of hackers called LulzSec Pilipinas, the National Privacy Commission of Philippines found that the Election Commission had violated the Data Privacy Act of 2012, and recommended criminal prosecution of its chairman, finding him liable when the agency failed to dispense its duty as a “personal information controller”.

It’s 2019, and that recommendation has still not been acted upon, because the National Privacy Commission of Philippines only has recommendatory powers for criminal prosecution. Meanwhile, data breaches continue at the Election Commission of Philippines.

Between 2017 and 2018, Aadhaar related personally identifiable data of several Indian citizens, including names, addresses, bank account numbers, in some cases pregnancy information and even religion and caste information of individuals, was published online by Indian government departments. The Centre for Internet and Society, in a report, estimated that personally identifiable data for 130-135 million Indian citizens had been leaked, thus putting them at risk. 210 government websites had made Aadhaar related data public, UIDAI confirmed in response to an RTI in 2017.

No one was held liable. There was no data protection law, no data protection authority, no criminal prosecution was recommended. Around that time, the Indian government was instead arguing in the Supreme Court that privacy isn’t a fundamental right under the Indian Constitution. Illustration: Ajit Ninan

What we can learn from these two instances is that for the enforcement of a citizen’s right to privacy, and ensuring that no one takes the protection of data lightly, there needs to be a strong privacy law that holds even the government responsible, and above all, a strong data protection authority that is independent and has powers to penalise even government officials. On some of these counts, the Personal Data Protection Bill, 2019, disappoints.

First, members of the Data Protection Authority will no longer be appointed by independent entities from diverse backgrounds: where they were previously going to be appointed by a committee comprising the Chief Justice of India or a Supreme Court judge, the Cabinet secretary, and an independent expert, the power to appoint members to DPA now rests solely with government officials, including the appointment of adjudicating officers. In addition, the central

government, in the interest of “national security, sovereignty, international relations and public order, can issue directions to DPA, which DPA will be bound by. Powers of DPA have also been reduced: while in the previous version of the bill, DPA had the sole power to categorise data as sensitive personal data, in the current version, the power rests with the central government, albeit in consultation with DPA. The central government will also notify any social media company as a significant data fiduciary, and not DPA. Only the central government can determine what critical personal data is, and not DPA.

This dependence on the government for appointments, functions and definitions, will invariably impact the independence of DPA, and even though the 2019 version of the bill gives it the authority to fine the state a maximum of Rs 5-15 crore, depending on the offence, i’d be surprised if this ever happens.

The bill does create significant exceptions for the state to acquire and process data, and an opportunity to create a base for surveillance reform in the country has been lost. The previous version of the bill had brought some sense of safety against mass surveillance, when it included the condition that processing of data by the government must be “necessary and proportionate”, drawing from Supreme Court’s historic right to privacy judgment. This is particularly important given that the bill also gives power to the government to exempt any agency from the provisions of the bill for processing of personal data, which includes acquiring data from any public or private entity.

Effectively, this means that government agencies may be exempt from any scrutiny by DPA, and can even collect data from third parties (for example, fin-tech companies, health-tech startups) without the user even knowing. Forget recommending criminal prosecution for mass surveillance, India’s DPA won’t even be able to fine a government agency for such a violation of the fundamental right to privacy. The government also has vast exceptions for data processing: “for the performance of any function of the state authorised by law”.

This aside, one of the more curious clauses in the bill is around non-personal data. The government, a few months ago, constituted a committee led by Infosys co-founder Kris Gopalakrishnan to look into the governance of non-personal data. Non-personal data, as the term suggests, is any data that is not related to an individual. In the bill, the government has given itself the right to acquire this data, which is essentially a company’s intellectual property, to “promote framing of policies for digital economy”. Why non-personal data finds a mention in a Personal Data Protection Bill is beyond comprehension, and this move will not inspire much confidence in businesses operating in India, when the state claims eminent domain over intellectual property.

It’s unfortunate minister Ravi Shankar Prasad is sending the bill to a select committee, given the fact that such significant changes to the bill should have led to another public consultation.

December 11, 2019 Nikhil Pahwa in TOI

ARE YOU READY FOR INDIA'S DATA PROTECTION LAW?

The Personal Data Protection Bill, 2019 (“**PDP Bill**”) was introduced in Parliament on 11 December 2019. If passed, the law will require organisations to revamp their data-related processes and embed privacy within their systems and operations. Here is a brief introduction to the law with a rundown of action items for organisations.¹

▪ How will organisations be affected by the law?

Any organisation that collects, uses, stores, shares or otherwise processes ‘personal data’ will be affected. An organisation will have to assess its existing data processing activities and implement changes to comply with the law. Additionally, the government may ask any organisation to provide its ‘anonymised’ personal data or ‘non-personal data’ for specific policy goals.

Action Item
<p>Understand if you are an organisation that processes personal data. Ensure preparedness for the law being passed, through the following:</p> <ul style="list-style-type: none"> ➤ Identify if you are a ‘data fiduciary’ or a ‘data processor’. A data fiduciary decides the purpose and means of processing. A data processor processes data on behalf of a data fiduciary. ➤ Identify if you are a ‘significant data fiduciary’ (notified by the Data Protection Authority (“DPA”) to be established under the forthcoming law). ➤ Make sure relevant teams within the organisation are aware of the law, including business, product, finance, legal/compliance/policy, human resources and communications/marketing/PR. ➤ Prepare your board of directors about anticipated changes. Make sure they understand that implementing privacy programmes may involve significant investments but are also advantageous and increasingly important for businesses. ➤ Prepare a comprehensive data inventory. ➤ Assess if you need to hire trained privacy personnel.

▪ What data is covered by the law?

Any data that can identify an individual, directly or indirectly, is covered. Examples: names, addresses, financial data and health data. IP addresses, web cookies and device IDs are also personal data if they can identify an individual. The individual is called ‘data principal’.

The PDP Bill has a separate category of data known as ‘sensitive personal data’ (“**SPD**”), for data that carries a higher risk of processing. Processing SPD has stricter compliance requirements. SPD includes financial data, health data, official identifiers and biometric data.

Action Item
Categorise all data collected and used by different departments of your organisation. Identify data that relates to individuals, directly or indirectly. Identify whether any of it is SPD.

▪ What should an organisation do before collecting and using individuals' data?

To process any personal data (collect, store, use or disclose), data fiduciaries will have to ensure that the processing takes place under one of these grounds or bases:

1. Processing based on consent of the data principal
2. Processing under a law or a court order
3. Processing for purposes related to employment
4. Processing for a ‘reasonable purpose’ specified by the DPA. This may include the operation of search engines, fraud prevention, mergers and acquisitions, and credit scoring.

Action Item

¹ Note: This is based on the draft Personal Data Protection Bill, 2019 circulated to members of parliament.

Before processing personal data, make sure you have identified a ground or basis for processing. Your organisation should be able to justify any act of processing under one of the listed bases.

▪ **How should an organisation take consent of a data principal?**

Consent should be free, informed, specific, clear and capable of being withdrawn.

Action Item
<ul style="list-style-type: none"> ➤ Inform individuals why you need their data and how you will use it, through a privacy notice. Ensure the privacy notice is clear and concise, such that a lay person will understand it. Include (a) purpose of collection; (b) identity/ contact details of data fiduciary; (c) basis of processing; (d) recipients; (e) time period of storage; (f) source of collection and, (g) access and rectification rights, among other things. Consider getting creative about your privacy notices, for example, through infographics. ➤ Get meaningful, affirmative action for consent. ➤ Allow individuals to withdraw consent with ease.

▪ **Are any other organisational measures/ controls required to be adopted?**

Organisations may have to:

- Prepare a privacy by design policy for a system-wide approach to data protection
- Undertake data protection impact assessments when using new technologies or processing that carries risk of significant harm
- Have organisational policies and conduct data audits annually
- Implement security safeguards
- Appoint a data protection officer

Action Item
<ul style="list-style-type: none"> ➤ Categorise all existing data and map data flows. ➤ Identify privacy and security risks. ➤ Frame policies to minimise those risks and embed privacy into organisational processes.

▪ **What rights does a data principal have over her personal data? How should an organisation enable these?**

A data principal can:

- Seek confirmation that the data fiduciary is processing her personal data
- Seek their personal data held by an organisation and a summary of processing activities
- Seek a list of all data fiduciaries with whom the data is shared
- Obtain correction of inaccurate data or updating data that is out of date
- Ask for data in a machine-readable format and have it transferred to a different entity (data portability)
- Restrict or prevent disclosure of her personal data by a fiduciary

Action Item
Adopt processes and implement technical capabilities to receive, review and respond to such requests.

▪ **Can personal data be transferred outside India? Can it be stored anywhere?**

An organisation can transfer and store personal data outside India freely. However:

SPD must be stored only in India, though it can be transferred outside India in limited ways:

- through contracts or intra-group schemes approved by the data protection authority
- when the transfer is to a ‘whitelisted’ country/ sector/ international organisation, approved by the central government
- when the transfer is approved by the DPA

Critical personal data (a list to be specified by the central government) must be stored and processed only in India. It can only be transferred outside India:

- to a person engaged in providing health/ emergency services where the transfer is needed for prompt action
- to a country/ sector/ international organisation, approved by the central government

Action Item
➤ Identify whether any data held by your organisation is critical personal data or sensitive personal data. ➤ Identify whether the transfer is permissible under any of the bases.

▪ **Are there penalties for non-compliance?**

Significant penalties can be imposed for violations:

- Maximum penalty is INR 15 crore or 4% of total worldwide turnover of the organisation

ABOUT IKIGAI LAW

Ikigai Law is a law and policy firm sharply focused on technology and innovation. We specialize in representing technology businesses, investors, and start-ups, to more mature companies focused on new business models. We work with our clients on regulatory and policy issues, private equity and venture capital investment transactions, mergers and acquisitions and other commercial transactions, intellectual property, and disputes. Our work is at the intersection of law, policy, regulation, technology and business, engaging with key issues such as [data protection and privacy](#), [fin-tech](#), [online content regulation](#), [platform governance](#), digital competition, [digital gaming](#), cloud computing, net neutrality, [health-tech](#), [blockchain](#) and [unmanned aviation](#) (drones), among others. Our key awards and recognitions include:

- Recognised TMT Practice – Chambers and Partners
- Boutique Law Firm of the Year 2019 – Asian Legal Business
- Law Firm of the Year – Mid Size 2019 by Idex Legal
- “Influential, knowledgable and effective” – Legal500
- Best Legal Advisor to Startups 2019 by Idex Legal

CHECKLIST: PERSONAL DATA PROTECTION LAW

1. INTRODUCTION

- The Personal Data Protection Bill, 2019 (“**PDP Bill**”) was introduced in Parliament on 11 December 2019. If passed, the law will require organisations to revamp their data-related processes and embed privacy within their systems and operations.
- Accountability is a key feature of the PDP Bill and organisations should be prepared to demonstrate compliance with its requirements. The PDP Bill proposes significant penalties for non-compliance that could go up to 4% of total worldwide turnover of an entity.
- The PDP Bill establishes a new regulator – the Data Protection Authority of India (“**DPA**”) – that is entrusted with enforcing this new law and ensuring compliance.
- This checklist is intended to be a starting point for organisations to understand their obligations under the law. The checklist lists out compliance requirements and action items for organisations under five heads: (i) understanding scope and preparing for the law; (ii) accountability; (iii) fair and lawful processing; (iv) data principals’ rights; and (v) transferring data outside India. The checklist indicates whether a set of actions is relevant for data fiduciaries (data controllers) (“**DFs**”) or data processors (“**DPs**”) or both. It also identifies the relevant teams that need to be involved in each set of actions:

Legal/ Compliance 

Technical and IT 

Customer Relations 

Public Relations 

HR 

2. COMPLIANCE CHECKLIST

(I) UNDERSTANDING SCOPE AND PREPARING FOR THE LAW

Subject	Description of PDP Bill requirement	Action	Relevant PDP Bill provision
Scope (DF/DP)	<p>The PDP Bill applies to the processing of ‘personal data’. Processing means collection, use, storage, sharing or any other activity related to data.</p> <p>The PDP Bill regulates data-processing activities of ‘data fiduciaries’ and ‘data processors’.</p>	<p>Organisations should:</p> <ul style="list-style-type: none"> ▪ Identify if they process any personal data (i.e. data that relates to an individual or can identify an individual). ▪ Understand if they determine the purpose and means of data processing. If so, they will be data fiduciaries. ▪ Understand if they are only processing data on behalf of another entity. In that case, they may be data processors. ▪ Identify if their data processing activities are exempted under the law. 	Clauses 2, 26

	<p>‘Significant data fiduciaries’ are required to comply with heightened obligations, such as conducting data protection impact assessments, appointing a data protection officer, record-keeping, and having their processes audited yearly. Social media intermediaries are classified as ‘significant data fiduciaries’ under the PDP Bill.</p>	<ul style="list-style-type: none"> ▪ Understand if they are ‘significant data fiduciaries’ (notified by the DPA). 	
● Territorial scope (DF/DP)	<p>The PDP Bill applies to data processing in India and to processing by Indian entities.</p> <p>The PDP Bill applies to processing outside India if it is in connection with any business carried out in India, or the systematic offering of goods or services in India; or in connection with any activity that involves profiling of data principals in India.</p> <p>The central government can exempt certain data processors from the law, where pursuant to contracts with offshore entities, data processors process data of individuals who are outside India.</p>	<p>Organisations should:</p> <ul style="list-style-type: none"> ▪ Identify if any part of their data processing activity takes place in India. ▪ If they process data outside India, identify if Indian citizens are involved or if the activity is conducted in connection with any business in India or offering of goods and services in India. 	Clauses 2, 37
● ● ● ● Data inventory (DF/DP)	<p>Significant data fiduciaries are required to keep records of important operations in the data life cycle.</p> <p>While not specifically required, several provisions such as privacy by design, data protection impact assessment, etc. will start with the preparation of a data inventory and mapping data flows. An inventory is the first step towards compliance with the PDP Bill.</p>	<p>Organisations should:</p> <ul style="list-style-type: none"> ▪ Identify all data processed and held within different departments, including details such as its source, who it will be shared with, who has access to it within the organisation, etc. ▪ Create a comprehensive data inventory using this information. ▪ Consider using automated privacy tools for preparing a data inventory. ▪ Develop processes for updating the inventory periodically. ▪ Understand different types of data with the organisation, such as ‘personal data’, ‘sensitive personal data’, ‘critical personal data’ and ‘non-personal data’. 	Clause 28

Non-personal data ● (DF/DP)	While most compliance requirements relate to personal data, data fiduciaries and processors can be asked by the central government to share anonymised or non-personal data for specific policy goals.	Organisations should: <ul style="list-style-type: none"> Understand types of non-personal data they hold and process. Develop processes to respond to government directions for non-personal data. 	Clause 91
---------------------------------------	--	--	-----------

(II) ACCOUNTABILITY

Accountability: Governance and Systems

Subject	Description of PDP Bill requirement	Action	Relevant PDP Bill provision
Privacy by design policy ● ● (DF)	Data fiduciaries should prepare a privacy by design policy. They may get this certified by the DPA. Once certified, they will be eligible to participate in a sandbox proposed under the PDP Bill. Through this privacy by design policy, they should embed privacy features in their systems and adopt suitable organisational and technical systems.	Organisations should: <ul style="list-style-type: none"> Develop a privacy by design policy. Develop procedures to identify risk of harm to data principals and formulate mitigation strategies. Ensure data protection obligations (such as purpose limitation, collection limitation, data quality and data storage) are reflected in business practices and in IT systems. Employ technology that is in accordance with commercially accepted or certified standards. Develop and implement processes to train personnel across all levels to ensure they understand data protection principles and PDP Bill requirements. Ensure privacy features are embedded into all parts of a data life cycle. 	Clause 22
Data protection impact assessment ● ● (DF)	Before undertaking certain processing activities, significant data fiduciaries are required to conduct a data protection impact assessment (“DPIA”). The activities for which a DPIA is required: processing involving new technologies or large scale profiling or use of sensitive personal data, or processing which carries	Organisations should: <ul style="list-style-type: none"> Create internal processes to ensure that privacy risk is understood as a business risk in the development of a product and the appropriate teams are flagged when a product involves an activity that requires a DPIA. Develop processes for conducting DPIAs and assign responsibility to relevant personnel. Develop templates for DPIA reports. 	Clause 27

	<p>a significant risk of harm to data principals.</p> <p>(The DPA will decide whether all organisations have to comply with this requirement or only significant data fiduciaries.)</p>		
Security safeguards ● ● (DF/ DP)	<p>Data fiduciaries should adopt appropriate security safeguards, after considering the nature and purpose of processing, risks associated with the processing, and likelihood and severity of harm that could arise from processing.</p> <p>(The DPA may issue standards for security safeguards to be maintained by data fiduciaries and data processors.)</p>	<p>Organisations should:</p> <ul style="list-style-type: none"> ▪ Develop procedures to assess risks associated with processing and the likelihood and severity of harm to individuals from their data-processing activities. ▪ Develop procedures to mitigate those risks using appropriate security safeguards. ▪ Include appropriate techniques such as de-identification, encryption, identity and access management, data loss prevention, as required. ▪ Undertake review of security safeguards periodically. ▪ Ensure third party contracts have appropriate security controls. ▪ Review security safeguards periodically and maintain a record of the review. 	Clause 24
Data audits ● ● (DF)	<p>Significant data fiduciaries should have their policies and processing activities audited annually by an independent data auditor.</p> <p>(The DPA will decide whether all organisations have to comply with this requirement or only significant data fiduciaries.)</p>	<p>Organisations should:</p> <ul style="list-style-type: none"> ▪ Develop processes to enable third party audits. ▪ Develop internal processes to demonstrate compliance with obligations under the PDP Bill. 	Clause 29
Grievance redressal ● ● ● (DF)	<p>Data fiduciaries should have effective grievance redressal mechanisms.</p>	<p>Organisations should:</p> <ul style="list-style-type: none"> ▪ Create mechanisms for data principals to raise grievances with the organisation and receive timely responses. ▪ Designate officers who will be the points of contact for such grievances. 	Clause 32

Breach notification     (DF)	Data fiduciaries should notify the DPA of a breach where such breach is likely to cause harm to a data principal.	Organisations should: <ul style="list-style-type: none"> ▪ Develop data breach response procedures to notify the DPA as soon as possible in case of a breach. ▪ Put in place procedures to assess situations exposing data principals to risk of harm. ▪ Prepare templates for notifying the DPA and data principals (when directed by the DPA). ▪ Review contracts with third parties and processors to ensure the fiduciary will be able to notify the DPA in time. ▪ Review liability provisions in third party contracts for breaches caused by third parties. ▪ Review insurance coverage for data breaches. 	Clause 25
--	---	--	-----------

Accountability: Personnel

Subject	Description of PDP Bill requirement	Action	Relevant PDP Bill provision
Personnel  (DF)	While not a specific requirement, several obligations under the PDP Bill require personnel to be adequately trained. For instance, privacy by design requires data fiduciaries to ensure that managerial, organisational and business practices are designed to anticipate and avoid harms to data principals.	Organisations should: <ul style="list-style-type: none"> ▪ Ensure that senior management is aware of the compliance requirements and impact of non-compliance. ▪ Allocate budget for data protection compliance. ▪ Consider having clear lines of reporting and allocation of responsibility for data governance within the organisation. ▪ Implement programmes to train personnel on data protection compliance requirements under the law and concepts such as harm and risk to individuals as a result of processing. 	Clause 22
Data protection officer  (DF)	Significant data fiduciaries should appoint data protection officers to ensure compliance with the PDP Bill and act as a point of contact for the data principal and the DPA.	Organisations should: <ul style="list-style-type: none"> ▪ Understand if they are a significant data fiduciary or are otherwise required to appoint a data protection officer. ▪ If required, appoint a data protection officer as the point-of-contact for all data compliance related issues. ▪ Ensure that the data protection officer resides in India. 	Clause 30

	(The DPA will decide whether all organisations have to comply with this requirement or only significant data fiduciaries.)		
--	--	--	--

(III) FAIR AND LAWFUL PROCESSING

Subject	Description of PDP Bill requirement	Action	Relevant PDP Bill provision
Basis for processing personal data ● ● (DF)	Any processing should be conducted under one of the legal bases/ grounds specified. These include consent, state action, legal obligation, compliance with court order, emergencies, employment and reasonable purposes to be specified by the DPA.	Organisations should: <ul style="list-style-type: none"> ▪ Identify and document a legal basis for processing any category of data. ▪ Before relying on consent, understand if any of the other bases are applicable. For instance, if personal data has to be shared under a law or for compliance with a court order, separate consent would not be required. ▪ Explain the bases of processing in their privacy policies/ notices. 	Chapter III
Consent ● ● ● (DF)	In order to lawfully process personal data, data fiduciaries must comply with strict consent requirements. They should obtain consent that is informed, free, clear and specific. In case of sensitive personal data, obtain ‘explicit’ consent.	Organisations should: <ul style="list-style-type: none"> ▪ Ensure that consent is sought before processing. ▪ Determine what makes consent ‘explicit’. ▪ Maintain clear records of consent obtained from data principals to be able to demonstrate that consent was given at the time of processing. ▪ Ensure that provision of goods or services or performance of a contract is not conditional on consent to processing any personal data that is not necessary for that purpose. ▪ Ensure that consent is free, specific and clear. ▪ Review existing consents to ensure compliance with the new requirements and where non-compliant, draft new consent forms to seek fresh consent. ▪ Create mechanisms to allow data principals to withdraw consent. ▪ Create mechanisms to allow data principals to give or withdraw consent through consent managers. 	Clauses 11, 23
Privacy notice ● ● ●	Data fiduciaries should notify data principals of: type of data collected, manner of collection, purpose of	Organisations should: <ul style="list-style-type: none"> ▪ Review and update privacy notices to make them PDP Bill-compliant (or develop privacy notices where they do not exist). 	Clauses 7, 23

(DF)	collection, likelihood of significant harm, procedure for exercise of data principal rights, among other things.	<ul style="list-style-type: none"> ▪ Develop processes to provide information in a clear and easily comprehensive form. 	
'Reasonable purpose' as a legal basis for processing ● ● ● (DF)	Data fiduciaries can process personal data if the processing is necessary for 'reasonable purposes' specified by the DPA. These may include mergers and acquisitions, network and information security, debt-recovery and fraud prevention.	<p>Organisations should:</p> <ul style="list-style-type: none"> ▪ Understand if processing is for any of the reasonable purposes specified by the DPA. ▪ Assess whether processing is 'necessary' for a listed reasonable purpose, having regard to factors such as interest of the data fiduciary in that processing, any public interest in processing, and the reasonable expectation of the data principal with respect to the processing. ▪ Record the assessment to be able to demonstrate compliance. 	Clause 14
Children's data ● ● ● (DF)	Data fiduciaries should process children's personal data in a manner that protects their interests and implement appropriate mechanisms for age verification and parental consent. The DPA may designate certain data fiduciaries who process large volumes of data relating to children as 'guardian fiduciaries'	<p>Organisations should:</p> <ul style="list-style-type: none"> ▪ Identify proportion of personal data likely to be of children and assess possibility of harm to children arising out of processing. ▪ Develop appropriate methods to verify age. ▪ Create forms for seeking parental consent. 	Clause 16

(IV) DATA PRINCIPALS' RIGHTS

Subject	Description of PDP Bill requirement	Action	Relevant PDP Bill provision
Right to confirmation and access ● ● ● (DF)	Data fiduciaries should provide clear and concise confirmation and summary of personal data processing activities and the list of data fiduciaries with whom the personal data has been shared.	<p>Organisations should:</p> <ul style="list-style-type: none"> ▪ Develop processes to allow individuals to make such requests. ▪ Create templates for summaries of personal data and processing activities to be provided to data principals, upon request. ▪ Consider automated means to provide confirmation and summary of processing activities to data principals. ▪ Maintain a list of entities with whom the personal data of is shared. 	Clause 17

Right to seek correction (DF)	Data fiduciaries should enable data principals to seek rectification or completion of their personal data.	Organisations should: <ul style="list-style-type: none"> ▪ Develop internal processes that enable correction of inaccurate data, completion of incomplete data, and update old data in a timely manner. ▪ Create a system whereby relevant stakeholders are notified of any change to the data pursuant to such requests. ▪ Understand the legal mechanisms under which these rights can be resisted. ▪ Develop templates which list the reasons for denial of such requests. 	Clause 18
Right to data portability (DF)	Data fiduciaries should provide and transmit personal data collected through automated means to a data principal or another data fiduciary in a machine-readable format.	Organisations should: <ul style="list-style-type: none"> ▪ Classify personal data according to automated processing and non-automated processing. ▪ Assess different machine-readable formats. ▪ Develop processes to enable secure data transfer to other data fiduciaries. ▪ Understand the legal mechanisms under which such requests can be resisted. 	Clause 19
Right to be forgotten (DF)	Data fiduciaries should restrict or prevent disclosure of personal data of individuals, if required to do so by the adjudicating officer.	Organisations should: <ul style="list-style-type: none"> ▪ Develop processes to determine the relevance of the data to the purpose of collection. ▪ Inform other stakeholders that the data principal has requested the erasure of personal data. 	Clause 20

(V) TRANSFERRING DATA OUTSIDE INDIA

Subject	Description of PDP Bill requirement	Action	Relevant PDP Bill provision
Data localisation (DF/DP)	Data fiduciaries should: (i) store sensitive personal data in India (but they can transfer such data outside India under limited legal bases); (ii) store and process critical personal data only in India.	Organisations should: <ul style="list-style-type: none"> ▪ Identify where data resides and review the residency practices. ▪ Ensure local processing and storage of critical personal data. ▪ Ensure local storage of sensitive personal data. 	Clause 33

● (DF/DP)	<p>Cross-border transfers</p> <p>Data fiduciaries may transfer sensitive personal data outside India under limited bases, which include: contract/ intra-group transfers approved by the DPA; transfers to countries/ sectors with adequate protection (permitted by the central government); or transfers specifically approved by the DPA. Transfers would also require explicit consent of the data principal as a necessary precondition.</p>	<p>Organisations should:</p> <ul style="list-style-type: none"> ▪ Review processes for cross-border transfers. ▪ Develop specific processes to conduct transfer of sensitive personal data. ▪ Ensure that explicit consent is obtained before transferring data outside India. ▪ Prepare contracts/ intra-group schemes and have them approved by the DPA. ▪ Consider preparing a template for request for specific approval from the DPA. ▪ Formulate country-specific processes for cross-border transfers. 	Clause 34
---	---	---	-----------

This checklist is intended as an overview of key action items for compliance with the personal data protection law. This should not be construed as, or relied upon, as legal or professional advice.

ABOUT IKIGAI LAW

Ikigai Law is a law and policy firm sharply focused on technology and innovation. We specialize in representing technology businesses, investors, and start-ups, to more mature companies focused on new business models. We work with our clients on regulatory and policy issues, private equity and venture capital investment transactions, mergers and acquisitions and other commercial transactions, intellectual property, and disputes. Our work is at the intersection of law, policy, regulation, technology and business, engaging with key issues such as [data protection and privacy](#), [fin-tech](#), [online content regulation](#), [platform governance](#), digital competition, [digital gaming](#), cloud computing, net neutrality, [health-tech](#), [blockchain](#) and [unmanned aviation](#) (drones), among others. Our key awards and recognitions include:

- Recognised TMT Practice – Chambers and Partners
- Boutique Law Firm of the Year 2019 – Asian Legal Business
- Law Firm of the Year – Mid Size 2019 by Idex Legal
- “Influential, knowledgeable and effective” – Legal500
- Best Legal Advisor to Startups 2019 by Idex Legal

Dvara Research | Policy Brief | October 2019

Implementing the Personal Data Protection Bill:

Mapping Points of Action for Central Government and the future Data Protection Authority in India

Authors: Srikara Prasad, Malavika Raghavan, Beni Chugh & Anubhutie Singh¹

Summary

The Central Government and the future Data Protection Authority (DPA) will face the complex task of notifying several rules and regulations in order to bring India's Personal Data Protection Bill (the Bill) into full effect. In the absence of such regulations, even if the Bill is enacted it could have limited impact and effect. There is a pressing need for a clear blueprint of how Central Government and the DPA will work together to systematically release regulation to bring to life the provisions of the Bill. A systematic approach could prevent the ad-hoc passage of rules which could create severe disruptions in the data economy and gaps in consumer protection.

In this policy brief, we set out the actions required from Central Government and the future DPA following enactment of the Bill. These actions are sequenced in order of priority based on our analysis of the interlinkages of sections within the Bill and the practical requirements of any data protection regime. The sequencing is aimed at ensuring that the main elements of the law come into effect without compromising consumer protections and inducing business uncertainty. This initial blueprint aims to drive forward the conversation on effective implementation, capacity and enforcement for India's future data protection regime taking into account our unique context.

¹ The authors work with Dvara Research, Mumbai, India. Our team benefitted from the intellectual engagement of Mr. Rahul Matthan throughout the development of this work. We thank him for his nuanced consideration of our views and rigorous peer review.

Introduction: Subordinate legislation under the draft Personal Data Protection Bill

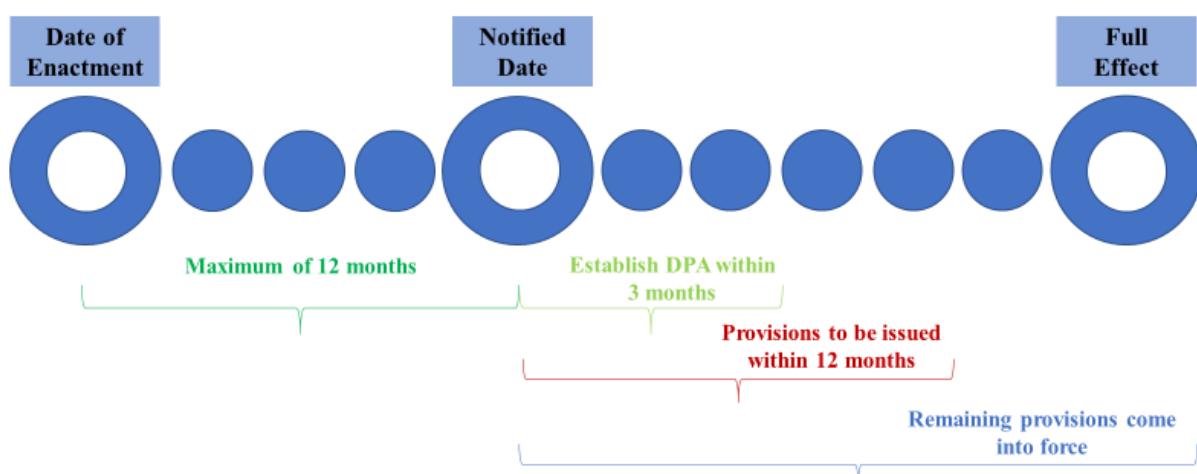
The draft Personal Data Protection Bill (the Bill) was released in July 2018 and followed by public consultation by the Ministry of Electronics and Information Technology (MeitY). If the Bill is passed by the Indian Parliament, it will result in the creation of an independent Data Protection Authority (DPA) entrusted with enforcing and overseeing the data protection regime in the country. The Central Government and the future DPA would then face the complex task of notifying several subordinate rules and regulations in order to bring the Bill into full effect.

This rule-making is critical for the effectiveness of the new data protection regime since the draft Bill defers several key details to be fleshed out in future regulations of the DPA. In the absence of such regulations, even if the Bill is enacted, it could have limited impact and effect. There is a pressing need for a clear blueprint of how the Central Government and the DPA will work together to systematically release regulation to bring to life the provisions of the Bill.

Through this policy brief, we seek to set out the actions that will be required from Central Government and the future DPA following enactment of the draft Bill in order to give it full effect. They are sequenced in order of priority based on our analysis of the interlinkages of sections within the Bill and the practical requirements of any data protection regime. The sequencing is aimed at ensuring that the main elements of the law come into effect without compromising consumer protection and inducing business uncertainty.

An assessment of the timelines in the draft Bill reveals that subordinate regulations on the various aspects of data protection need to be issued by Central Government and the DPA within an outer limit of **two and a half years** from the date of the enactment of the draft Bill.² This is represented pictorially below and explained in Table 1.

Figure 1: Timelines for issuing subordinate legislation under the draft Bill



² S.97, (Chapter XIV- Transitional provisions), The Personal Data Protection Bill, 2018.

Section I of this brief summarises some of the timelines indicated in the draft Data Protection Bill 2018. Section II sets out the actions of the Central Government that need to be performed in the period between enactment of the law and from three months of the notified date. Section III sets out the actions that the DPA must perform following its establishment.

I. Timelines for implementation under the draft Personal Data Protection Bill

The key milestones and time periods (represented pictorially on page 1) to bring the future data protection law into force are summarized in the table below, as per section 97 of the draft Bill.

Table 1: Timelines for regulation-making under the draft Bill		
Milestone	Time period	Action for DPA/ Central Government in this time period
Date of enactment	Date on which the Act receives presidential assent.	The Central Government must specify a “notified date”.
Notified date	Date notified by the Central Government in the Official Gazette within 12 months of the date of enactment.	The following provisions take effect on the notified date: <ul style="list-style-type: none"> - transitional provisions (under Chapter XIV); - provisions to enable the operation of the DPA (Chapter X); - the Central Government’s power to make rules and the & DPA’s powers to make regulations (respectively) under the draft Bill.
Establishment of the DPA	Within 3 months from the notified date	Central government must establish the DPA.
	Within 12 months from the notified date	The DPA must issue regulations on: <ul style="list-style-type: none"> - issuing codes of practice on different matters;³ - grounds of processing personal data for reasonable purposes (s 17).⁴
Full effect	Within 18 months from the notified date.	All remaining provisions automatically come into effect 18 months from the notified date.

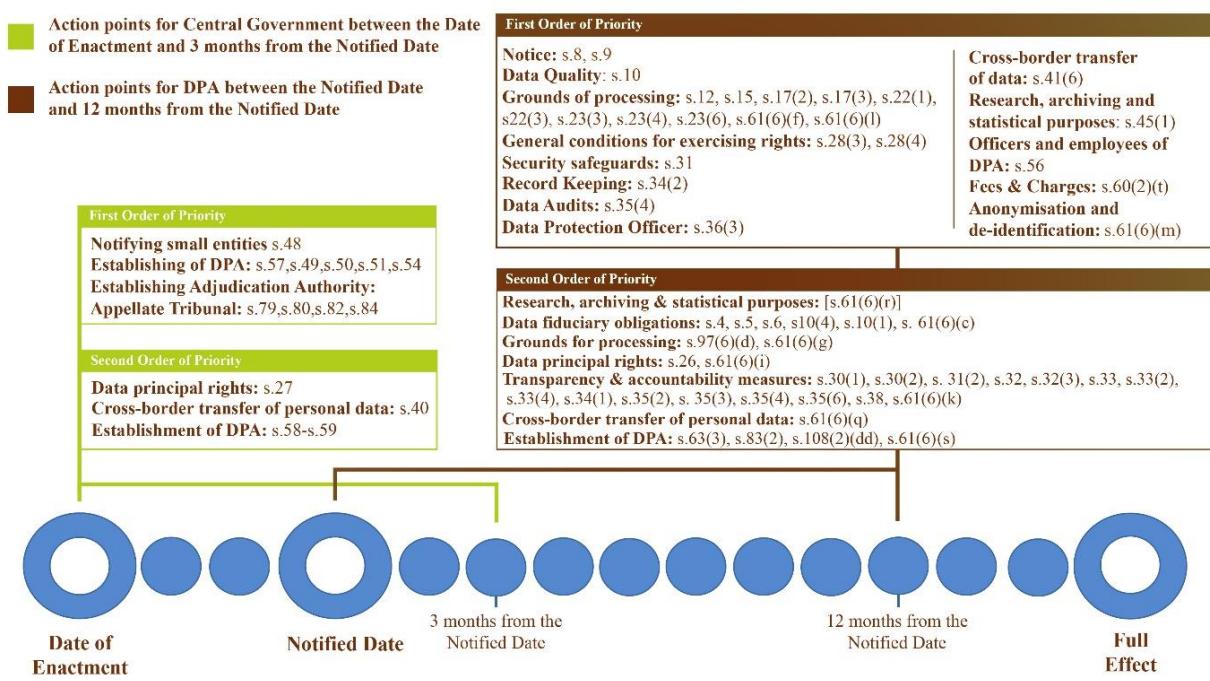
From this table, it becomes clear that after the Date of Enactment of the Bill, immediate actions will be required from the Central Government to establish the DPA, and subsequently to clarify the content of particular provisions. The DPA will also need to undertake a range of actions in the first 12 – 18 months of its establishment to give effect to the provisions of the Act.

³ The Personal Data Protection Bill, 2018, s.97(6).

⁴ The Personal Data Protection Bill, 2018, s.97(5).

This policy brief provides a blueprint of action points for the Central Government and the DPA to issue subordinate legislation. The blueprint is summarised in figure 2, which mentions all the rules and regulations which must be issued by the Central Government and the DPA. They are sequenced from left to right beginning at “Date of Enactment” and ending at “Full Effect.” The segment colour-coded in light green contains all the action points for the Central Government, which must be completed between the Date of Enactment and 3 months from the Notified Date. The segment colour-coded in brown contains all the action points for the DPA, which must be completed between the Notified Date and 12 months from the Notified Date.

Figure 2: Blueprint for issuing subordinate legislation by the Central Government & the DPA in India



The blueprint has been created after analyzing requirements of the draft Bill and the practicalities of implementation. The action points in the blueprint are sequenced into (A) first order of priority and (B) second order of priority for the Central Government and the DPA separately based on:

- particular provisions of the Bill which need subordinate regulation to take effect;
- consumer protection considerations and the need to have effective user rights after the date of enactment of the Bill;
- practical clarity required by data fiduciaries and controllers to comply with obligations under the Bill.

The blueprint does not attempt to provide a step-by-step process for issuing subordinate legislation but broadly highlights the order in which subordinate legislation may be issued. Section II and section III explain these action points in detail by highlighting the precise actions required from the Central Government and the DPA to systematically bring the Bill into full effect.

II. Subordinate legislation to be issued by the Central Government

The draft Bill tasks the Central Government to make **rules** (under section 107) and **notifications** (under different provisions). The powers and functions of the Data Protection Authority (DPA) are reliant on the issuing of rules by the Central Government. Certain key substantive provisions also require implementing rules to be issued by the Central Government. Central Government thus needs to begin taking action immediately from the Date of Enactment of the Bill. In the tables below we set out the rules and notifications required to be issued, sequenced as (A) first order of priority and (B) second order of priority to facilitate a smooth transition and implementation of the future Personal Data Protection Act.

A. Central Government – First Order of Priority ⁵		
Subject	Action Point	Tool
Scope & Limitations	Manual processing by small entities [s.48(2)(2)]: Prescribing the amount of annual turnover of an entity for it to qualify as a small entity	Rule [s.107(2)(f)]
Establishment of DPA	Grants by the Central Government [s.57]: Specifying the sums of money to be given to the DPA as thought fit for the purpose of this legislation	Provision [s.57]
	Incorporation of the DPA [s.49]: Notifying the place of establishment, location of the head office of the DPA	Rule [s.107(2)(g)]
	Appointment of DPA members [s.50]: Prescribing the composition and the qualifications of the DPA members	Notification [s.49(1)]
	Terms and conditions of appointment [s.51]: Specifying the terms and conditions for service of DPA chairperson and members, and their remuneration	Rule [s.107(2)(h)]
	Meetings of the DPA members [s.54]: Specifying the times and places, rules and procedures for meetings of the DPA	Rule [s.107(2)(i)]
Establishment of DPA – Adjudication Authority	Appointment of an Adjudicating Officer [s.68]: Specifying the qualification, manner, terms and conditions of appointment and jurisdiction of the Adjudicating Officer	Rules [s.107(2)(u)] and [s.107(2)(v)]
	Manner of adjudication [s.74]: Specifying the manner in which adjudicating officers will conduct an inquiry	Rule [s.107(2)(w)]
	Manner of filing a complaint with the Adjudication Wing [s.39(4)]: Prescription of the manner in which a Data Principal may file a complaint for grievance redressal	Rule [s.107(2)(c)]

⁵ As per s. 97(3), matters relating to Chapter X and s.107 will come into force on the notified date i.e. 12 months from the Bill's enactment. Therefore, the Central Government must deal with these matters as a priority.

	Manner of complaint and compensation to Data Principal after adjudication [s.75(2)]: Prescribing the form and manner in which a complaint may be instituted for adjudication and the compensation that may be offered	Rules [s.107(2)(x)] and [s.107(2)(y)]
	Codes of Practice [s.61]: Prescribing the procedure for issuing of Codes of Practice, the manner in which they may be modified or revoked and the manner in which they may be recorded	Rules under 107(2)(q), 107(2)(r) & 107(2)(s)
Appellate Tribunal	Establishment of the Appellate Tribunal [s.79(1), s.80, s.82]: Establishing an Appellate Tribunal, criteria for appointment and composition of the Tribunal, staff and their renumeration	Rules [s.107(2)(z)], [s.107(2)(aa)] & [s.107(2)(bb)]
	Appeals to the Appellate Tribunal [s.84]: Prescribing the form, manner and fee for filing an appeal or application before Appellate Tribunal	Rule [s.107(2)(cc)]

B. Central Government – Second order of priority

Subject	Action Point	Tool
Rights of Data Principals	Right to be Forgotten [s.27(4)]: Prescribing the manner and form for the application for exercising the Right to be Forgotten by Data Principals	Rule [s.107(2)(a)]
	Right to be Forgotten [s.27(5)]: Prescribing the manner in which orders of the Adjudicating officers may be applied for review with respect to the exercise of the right	Rule [s.107(2)(b)]
Cross-border transfer of personal data	Conditions for cross-border transfer [s.41(1)(b)]: Specifying of countries, or sector of countries or international organisations to which transfer of personal data is permissible	Rule [s.107(2)(d)]
	Conditions for cross-border transfer [s.41(4)]: Specifying the time period within which the DPA would be notified of cross-border transfer of personal data for emergencies under [s.41(3)]	Rule [s.107(2)(e)]
	Notification of Critical Personal Data [s.40(2)]: Notifying the categories of personal data as <i>critical personal data</i> that may only be processed within India	Notification [s.40(2)]
Establishment of the DPA	Accounts and Audits [s.58]: Prescribing the form in which accounts and annual statements will be recorded and the time intervals of account auditing of the DPA	Rule [s.107(2)(k)] and [s.107(2)(l)]
	Furnishing of returns, etc. to the Central Government [s.59]: Prescribing the form and manner in which returns, statements and particulars must be furnished to the Central Government	Rule [s.107(2)(m)]

III. Subordinate legislation to be issued by the Data Protection Authority

Most of the substantive provisions in the draft Bill need clear regulations and codes to be enacted by the future DPA to take effect. The draft Bill enables the DPA to issue **regulations** (under section 108), **notifications** (under different provisions) and **codes of practices** (under section 61) to strengthen and smoothen regulation under the future of data protection regime. Below we set out the actions to be taken by the DPA sequenced by those that need to be (A) first order of priority and (B) second order of priority, to give effect to the substantive provisions of the draft Bill.

A. DPA - First Order of Priority		
Subject	Action Point	Tool
Scope & Limitations	Anonymisation [s.3(3)] and De-identification [s.3(16)]: Providing methods of anonymisation and de-identification.	Codes of Practice [s.61(6)(m)]
	Research, Archiving or Statistical Purposes [s.45(1)]: Specifying the provisions which are not applicable to the processing of data for research, archiving or statistical purposes.	Regulations [s.108(2)(z)]
Data Fiduciary Obligations	Notice [s.8]: Prescribing information which data fiduciaries must provide in notices.	Regulations [s.108(2)(a)]
	Notice [s.8]: Issuing model forms and guidance.	Codes of Practice [s.61(6)(a)]
	Data Quality [s.9]: Prescribing measures for ensuring data quality.	Codes of Practice [s.61(6)(b)]
Grounds of Processing	Processing on the basis of consent [s.12]: Prescribing conditions for valid consent.	Codes of Practice [s.61(6)(d)]
	Processing necessary for prompt action [s.15]: Prescribing measures for processing data on this ground.	Codes of Practice [s.61(6)(e)]
	Processing for reasonable purposes [s.17(2)]: Specifying reasonable purposes for which personal data can be processed.	Regulations [s.108(2)(c)]
	Processing for reasonable purposes [s.17(3)]: Prescribing safeguards to protect the rights of data principals.	Notifications [s.97(5)]
	Processing for reasonable purposes [s.17(3)]: Specifying provisions of <i>Notice</i> (s.8) which are not applicable.	Regulations [s.108(2)(d)]
	Issuing codes of practice for activities for which personal data can be processed on this ground.	Codes of Practice [s.61(6)(f)]
	Further categories of sensitive personal data [s.22(1)]: Prescribing further categories of sensitive personal data and the grounds on which these categories of data can be processed.	Regulations [s.108(2)(e)]

	Further categories of sensitive personal data [s.22(3)]: Prescribing additional safeguards for categories of personal data collected for repeated, continuous or systematic collection for profiling.	Regulations [s.108(2)(f)]
	Processing children's data [s.23(3)]: Prescribing factors for determining the appropriateness of age verification mechanisms.	Regulations [s.108(2)(g)]
	Processing children's data [s.23(4)]: Notifying guardian data fiduciaries.	Notifications [s.23(4)]
	Processing children's data [s.23(6)]: Specifying modifications in the activities of guardian data fiduciaries who offer counselling or child protection services.	Regulations [s.108(2)(h)]
	Issuing codes of practice for processing of personal data of children and development of appropriate age-verification mechanisms and mechanisms for processing data on the basis of consent of users incapable of providing valid consent.	Codes of Practice [s.61(6)(h)]
Rights of Data Principals	General Conditions for Exercising Rights [s.28(3)]: Prescribing the time period within which a data fiduciary must comply with a data principal's request.	Regulations [s.108(2)(i)]
	General Conditions for Exercising Rights [s.28(4)]: Prescribing the time period & manner in which a data fiduciary must convey reasons for refusing the request and inform data principal about the right to file a complaint with the DPA.	Regulations [s.108(2)(j)]
Transparency & Accountability Measures	Security Safeguards [s.31(1)]: Prescribing standards for security safeguards to be maintained by data fiduciaries and data processors.	Codes of Practice [s.61(6)(l)]
	Record-Keeping [s.34(2)]: Prescribing the form in which records will be maintained by data fiduciaries.	Regulations [s.108(2)(r)]
	Data Audits [s.35(4)]: Prescribing eligibility, qualifications and functions of data auditors.	Regulations [s.108(2)(v)]
	Data Protection Officer [s.36(3)]: Prescribing eligibility and qualifications for data protection officers.	Regulations [s.108(2)(w)]
Cross-Border Transfer of Personal Data	Conditions for cross-border transfer [s.41(6)]: Prescribing the manner of certification and time period within which transfer of data under standard contractual clauses and intra-group schemes.	Regulations [s.108(2)(y)]
Establishment of the DPA	Officers and employees of DPA [s.56(1)]: Appointing officers, employees, consultants and experts.	Regulations [s.108(2)(aa)]
	Officers and employees of DPA [s.56(2)]: Prescribing remuneration, salary or allowances, terms and conditions of services.	Regulations [s.108(2)(bb)]
	Fees & Charges [s.60(2)(t)]: Prescribing fees and charges for carrying out purposes of the Act.	Regulations [s.108(2)(bb)]

B. DPA - Second Order of Priority

Subject	Action Point	Tool
Scope & Limitations	Issuing codes of practice for processing personal data/sensitive personal data to carry out any activity necessary for research, archiving or statistical purposes.	Codes of Practice [s.61(6)(r)]
Data Fiduciary Obligations	Fair and reasonable processing [s.4]: Providing guidance on what the DPA interprets as <i>fair and reasonable</i> .	Informal Guidance
	Purpose limitation [s.5]: Providing guidance on what the DPA interprets as <i>reasonable and incidental purpose</i> .	Informal Guidance
	Collection Limitation [s.6]: Providing guidance on what the DPA interprets as <i>necessary for purposes of processing</i> .	Informal Guidance
	Data storage limitation [s.10(4)]: Prescribing the manner in which data must be deleted.	Regulations [s.108(2)(b)]
	Data storage limitation [s.10(1)]: Prescribing the measures pertaining to data retention.	Codes of Practice [s.61(6)(c)]
	Prescribing the methods of destruction, deletion or erasure of data when required under the Act.	Codes of Practice [s.61(6)(c)]
Grounds for Processing	Issuing codes of practice for processing of personal data under Chapter III.	Codes of Practice [s.97(6)(d)]
	Issuing codes of practice for processing of sensitive personal data under Chapter IV.	Codes of Practice [s.61(6)(g)]
Rights of Data Principals	Right to data portability [s.26]: Prescribing standards and means to avail the right to data portability.	Codes of Practice [s.61(6)(j)]
	Issuing codes of practice for exercise of any right by data principals.	Codes of Practice [s.61(6)(i)]
Transparency & Accountability Measures	Transparency [s.30(1)]: Prescribing the form in which data fiduciaries must make information available to data principals.	Regulations [s.108(2)(k)]
	Transparency [s.30(2)]: Prescribing the manner in which the data fiduciary must notify data principals of important operations in the processing of personal data.	Regulations [s.108(2)(l)]
	Security safeguards [s.31(2)]: Prescribing the manner in which security safeguards must be periodically reviewed.	Regulations [s.108(2)(m)]
	Personal data breach [s.32(3)]: Prescribing the time period within which the data fiduciary must issue personal data breach notification to the DPA.	Regulation [s.32(3)]

Transparency & Accountability Measures	Personal data breach [s.32]: Prescribing the appropriate action to be taken in response to a personal data breach.	Codes of Practice [s.61(6)(o)]
	Data Protection Impact Assessment [s.33(2)]: Specifying the circumstances or classes of data fiduciaries or processing operations for which it is mandatory to conduct a Data Protection Impact Assessment.	Regulations [s.108(2)(n)]
	Data Protection Impact Assessment [s.33(2)]: Specifying the cases where the Data Protection Impact Assessment must engage a Data Auditor.	Regulations [s.108(2)(o)]
	Data Protection Impact Assessment [s.33(4)]: Prescribing the manner in which the DPIA report must be submitted to the DPA.	Regulations [s.108(2)(p)]
	Data Protection Impact Assessment [s.33]: Prescribing the manner in which DPIA must be carried out.	Codes of Practice [s.61(6)(p)]
	Record-keeping [s.34(1)]: Prescribing <i>other aspects of processing</i> for which records must be maintained.	Regulations [s.108(2)(q)]
	Record-keeping [s.34(1)]: Providing guidance on what the DPA interprets as <i>important operations in the data life-cycle</i> .	Informal Guidance
	Data Audits [s.35(2)]: Prescribing the factors which must be considered while evaluating compliance with stated provisions.	Regulations [s.108(2)(s)]
	Data Audits [s.35(2)(f)]: Prescribing the other matters with which data fiduciary's compliance should be evaluated.	Regulations [s.35(2)(f)]
	Data Audits [s.35(3)]: Prescribing the form, manner and procedure by which data audits must be conducted.	Regulations [s.108(2)(t)]
	Data Audits [s.35(6)]: Prescribing the criteria which will be used for rating data trust scores.	Regulations [s.108(2)(u)]
	Data Audits [s.35(4)]: Registering persons as data auditors.	Regulations [s.35(4)]
	Classification as significant data fiduciaries [s.38(1)]: Notifying certain data fiduciaries or classes of data fiduciaries as significant data fiduciaries.	Notifications [s.38(1)]
	Classification as significant data fiduciaries [s.38(2)]: Prescribing the manner in which significant data fiduciaries must register themselves with the DPA.	Regulations [s.108(2)(x)]
	Classification as significant data fiduciaries [s.38(3) & s.38(4)]: Notifying the obligations which will apply to different classes or kinds of data fiduciaries.	Notifications [s.38(3) & s.38(4)]
	Prescribing measures for transparency and accountability, including standards to be maintained by data fiduciaries and data processors under Chapter VII.	Codes of Practice [s.61(6)(k)]
Cross-Border Transfer of Personal Data	Issuing codes of practice for cross-border transfer of personal data under section 41.	Codes of Practice [s.61(6)(q)]

Establishment of the DPA	Power to call for information [s.63(3)]: Prescribing manner in which information shall be provided to the DPA.	Regulations [s.108(2)(cc)]
	Distribution of business amongst benches [s.83(2)]: Notifying distribution of the business of the Appellate Tribunal among benches, transfer of members between benches and provide for matters which may be dealt with by each bench	Notification [s.83(2)]
	Issuing rules and regulations in any other matter which the DPA views as required.	Regulations [s.108(2)(dd)] Codes of Practice [s.61(6)(s)]

Contact Us

Dvara Research, Chennai
10th Floor-Phase 1,
IIT-Madras Research Park,
Kanagam Village, Taramani
Chennai 600113

Dvara Research, Mumbai
The Mosaic, Raaj Chambers, 5th Floor,
New Nagardas Road,
Modra Pada, Andheri (E)
Mumbai 400053

E-mail: ffi@dvara.com

Twitter: [@dvararesearch](https://twitter.com/dvararesearch)

[@_FutureFinance](https://twitter.com/_FutureFinance)

Website: www.dvara.com/research/

Liveblog on Data Protection Consultation open house Delhi

We're liveblogging the data protection consultation discussion from Delhi. Comments are largely paraphrased. Please read in reverse chronological order.

[and we're done for today]

1533hrs: Naveen, STAR: What we believe is that most of the concerns are rising from the fact that most of the notices are highly complex. That will enable people to consent for allowing the usage of the data. Purpose limitation should be on the basis of what the consumer wants.

1537hrs: Usha Ramanathan: an accusation of rape or murder. If that gets found, or of someone is a witness or a complainant. we need the idea of proximity.

1537hrs: Justice Srikrishna: in a family court, a judge controls the proceedings. All reports are anonymised. Allegations will be there to understand, for posterity. That information is today protected.

1535hrs: You've mentioned the idea of some things that should not be digitised. One thing bothering me is digitisation of courts. When cases can filed, many things get said. Then it results in what it results in. Everything is getting into the digital space. It has huge implications for sociology of our country. Many statements are made and meant only for the courtroom. When they become a part of public commons it becomes dangerous.

1530hrs: Kamlesh Bajaj: There have been other judgments re EU GDPR, and talked about personal information on a company register. That should not be erased. Public interest should be larger than personal right in some cases.

1530hrs: Smitha Krishna Prasad, CCG at NLU Delhi: We have very limited comments today. We'd like to point out that any new data protection law would be crucial. We would urge the committee to be open and transparent and add members (civil society). This consultation in Delhi was with short notice, and before the deadline for the written submissions. We wanted to suggest more consultations, and with adequate notice. Consultations should be after the written submissions. The law commission has used this as well.

1528hrs: Usha Ramanathan: The data controllers liability should be even higher. It's more confusing regarding UIDAI because they decide.

1522hrs: [I made a point about confusion regarding ownership of data, and data as a right and data as a property]

1520hrs: We can look at a BCCC and the MIB, and the BCCC can ask for act

1511hrs: Raman Chima: The ATG has a right to access your data, when the challenges were made to DPAs. Matt Schrems case. The right to access your data must be in the regulatory regime. You can build on top of that as well.

Tehre's a basic to be able to access your data as a basic right. That should be subject to oversight, and right to make it portable, and a citizen focused right.

1514hrs: Nachiket: With regards to Aadhaar and RTI. The composition of the committee is a concern are on public record have made statements for Aadhar. and I would urge chairperson to get some balance by bringing in members of civil society. If we can have an additional round after the submissions, and a second round of consultations. I would like to share my personal experience with Aadhaar: I had to take an Aadhaar before the Aadhaar act was passed to register my marriage. No consent was taken from me. Subsequently when I've tried to revoke consent, which they state is possible, I've not been able to do it at the center or at the call center. In terms of how this will affect the Aadhaar act or IT act, some change needs to be made to bring grievance redressal.

From the point of view of RTI, an RTI was filed for the deliverances of the committee and meetings, I would request that the committee adhere to the highest standards of transparency.

1511hrs: Srinivas: I'm interested in predictive policing. Algorithms that are governing us need to be transparent and procedures need to be transparent.

1510hrs: Arghya Sengupta: you could stop any process which is automated. Second [missed this]. Third is that you have the right to know the algorithms.

1508hrs: Ajay Bhushan Pandey: What is the criteria a credit rating agency use? Tehre should be some adjudication and review. In some countries, it's not the monopoly of one company. The agency which does this fairly will survive, without disclosing the intellectual property.

1507hrs: Justice Srikrishna: If a traffic camera does this, then challenge it. A judge will ask for transparency. If you expect transparency in algorithms everywhere, then that won't work. The right thing to do is to go to an adjudicator.

1505hrs: Algorithms are discriminatory, but we don't know what governs them. The scoring systems for different insurance agents, I should have, as a citizen, have every right to know how these systems are designed. Especially inside the government. There are cases where police departments are using algorithms, but we have no idea. These are black boxes. Citizens should have a right to know what algorithms are governing us.

1505hrs: Justice Srikrishna: Fines have to be proportionate to the ability of the data controller, and be preventive.

1501hrs: Ambar Sinha, CIS: It would be worthwhile for us to look at the international experience of DPAs and ICOs in other countries. The UK office has used fines for enforcement. They've realised that where data controllers are putting in mitigation strategies, the fines need to be reduced. It's important in the legislation to empower the data protection authority. The powers have to be across a wide spectrum. The authority should have the power to receive complaints, and enforce based on orders that it passes. When it looks

at the pyramid of supports, whether it has privacy shields and trust marks, and carrying out audits of data controllers.

The other point: as far as the principles should be very very clearly in the primary legislation. When specific practices in sectors are concerned, there needs to be active participation from civil society and academia. It took the GDPR 10 years. In Netherlands, it took them 15 years to come up with sectoral codes. The DPAs should work with civil society and academia.

1458hrs: Ajay Bhushan Pandey: The liability should be proportionate to the damage done. If you look at the cost of the insurance. There will be some other company who will be more efficient and his cost of insurance will be much lower. A good driver will get insurance at a lower cost vs someone who is not a good driver.

1457hrs: Pankaj, Telenor: How will we define liability? If we have insurance then that increases the cost of doing business.

1454hrs: Justice Srikrishna: Take Bhopal tragedy, Uphaar tragedy. If there is a situation where extremely sensitive things are being handled, accountability has to be higher and there has to be proportionate liability. I'm not talking about criminal negligence. I'm talking about civil liability, and compensation. If there is a damage to the data subject, why is he or she not entitled to the compensation. That will be proportionate to the lack of accountability of the data controller. The approach can be insure yourself. Why can't this be an alternate way. I agree with Mrs Ramanathan, the law should be person centric.

1453hrs: Pankaj, Telenor: The right to edit and portability. We can't have a free for all here since there will be a huge cost. There has to be a fee mechanism. Something that needs to be there. On accountability of data controllers, accountability is required. There will be just lots of categories of data controllers around. The moment you talk about accountability, you'll go to liability, and the case which is given in the consultation paper, then any data controllers will survive. These issues need to be deliberated. There needs to be a limited liability defined.

1451hrs: Justice Srikrishna: What will be the adjudicating process? I'm telling you there needs to be a separate adjudication body. For example, stock exchange rules require trade defaults to be arbitrated by members. That's a better mechanism than a lok adalat.

1427hrs: Kamlesh Bajaj: Awareness creation is a massive exercise. Who will implement privacy programs in organisations. The key point has to be that the ombudsman, working with SROs. It would be verticals like DSCI in the IT industry, in banking it could be IBA. The way privacy laws were created, they were codes of practice were created by industry and then it became law.

[He talks about consumer court not working]

1426hrs: [I made a point about right to be forgotten, that it shouldn't be used

for censorship]

1439hrs: Should be independent. You want to make it partially transparent, have a criteria. I'll save this for submissions

1439hrs: Arghya Sengupta: how should public defenders be appointed?

1438hrs: Ramanjit Singh Chima: Seeing the sort of requests that are sent to LEA, there's a safeguard that is urgently required. Sometimes the home secretary is a buffer. Today a tech company has fewer protections than a telecom company.

1437hrs: Justice Srikrishna: In this country we've had stringent laws like TADA. But there were also preventive detention laws. What were the safeguards provided? There was post facto scrutiny. Would it be feasible to have pre-action scrutiny by a body put together, a committee.

1433hrs: Ramanjit Singh Chima, Access Now: The FISA process doesn't say that there's a blanketed exception for the government. California has a data protection regime. For law enforcement a separate regime applies in terms of what a FISA court can do.

The flaw in the process was that there wasn't a public defender. There needs to be someone saying that this may not be accurate that goes on record. IF there's a process of judicial process, we need a public defender. The UK passed a law that you can challenge a legal surveillance, and it has now said that certain warrants need to judicial approval. The EU court of justice has struck down data retention laws. There should be no blanket security exceptions. It's on the committee whether you want to put in a surveillance chapter.

1431hrs:

Justice Srikrishna: Have you look at the FISA court option? Do you think it would work if we had a situation where however agent the matter is, it has to be adjudicated by a judicial authority.

Usha: A secret court with secret orders is ineffective.

Justice Srikrishna: Let there be a judge at the rank of an SC judge?

Usha: It's more important to place it on record and there being a review, because someone who makes a wrong call can be held accountable.

1424hrs: Usha Ramanathan: one is where the state is treating all the data and our bodies. The eminent domain principle is also used to hand it over of private players. The other is

The third is national security, which is a type of immunities. In the AP shah committee report we struggled with national security. NAT GRID was supposed to be a pipeline. Then there was a presentation made to the cabinet, and the RTI was that it was about the project. It was delayed for 20-25 ays and then they said that it was a national security exception. All these agencies aren't just

beyond the law but also beyond parliamentary control. You need to identify a legal regime and a supervisory and accountability regime.

1425hrs: Justice Srikrishna: who determines national security? it's the executive. How does one neutralise the difficulty if the person at the top

1418hrs: Usha Ramanathan: I'm forced to come in when there's a statement like no law until we innovate. WE have a lot of experience when we look at the state resident data hubs. It's not about collecting what we want and keeping it safe. GSTN is also in private hands now. There is this ambition of using technology and creating wealth, about a trickle up philosophy of economics. It's appalling that people make this kind of statement. We don't need to assist in this trickle up. We have inequality growing, but now you're looking at trickle up, and to let people monetize this information. The RTI community has been very concerned. They've been asking for transparency. There's a distinction between state being transparent to people and people being transparent with state. We see this committee being constituted by people who support the UID project, and in the report we see

two of your members, we've had seen people arguing that privacy is not a fundamental right and arguing about it. The AP Shah committee was civil society. We would like for a committee to be credible, and for the report to be acceptable.

Yesterday when we had the massive breach of the UID database. It could be any database. It's unwise to bank only on those punishing those who misuse it. If the data controller has to be responsible and the data controller is responsible for deciding who is responsible. That should be avoided. These are things that you should keep out of any framework. Take lessons from what has happened. Yesterdays breach deserves a close study.

On the right to be forgotten, the point about what is happening now, is that technology makes many things possible that we want and do not want. when we don't want it, the idea of opting out becomes more complicated should be. These databases talk across time and across people and various kinds of activities. They leave no space for people to leave their past behind.

When we look at eminent domain. Data is entering the region of eminent domain. I'm not comfortable with my data entering the property domain, and it becomes property. The doctrine of eminent domain is entering the domain of data.

1415hrs: Mahesh Uppal, telecom consultant: I believe that in a sector such as this, and the scale of innovation, it would be extremely risky to lay down rigid positions. It's important that there's the issue of the data protection authority. Once we have that, if its driven by principle rather than detail, then it becomes incumbent that we have an authority. That would allow us to anticipate what happens in the future. Too detailed a legislation would be counter productive, not only for reasons of scale and innovation, but also it is dependent on assumptions made. These are all relatively difficult to establish,

and there's no way to argue, that just because something is localised in India, does it become more secure? Are we convinced that localised is secure, or something that is not localised is insecure. We must be driven by evidence of harm.

1410hrs: Praneet, TCS: [Missed most of his comments].

On data localisation, we should encourage data localisation, but we should allow cross border data flows.

GDPR can be a bit vague when it comes to right to be forgotten.

Data controller should be completely accountable. If there's a joint data controller, then there should be joint responsibility.

1406hrs: Apar Gupta: What should be the ambit of the statute and the power of the regulator. The TRAI as a regulator was able to fulfil the public interest in case of net neutrality. What is essential is to define common principles which should be enforced by the regulator: necessity and proportionality. With respect to mass surveillance, there are principles from Justice Nariman. Does PUCL standard hold well and good? We need a heightened standards, but what we need are principles first.

After comments, please have a counter comment period, and comments, and a consultation in person should be held.

1401hrs: Srinivas Kodali: When you've classified only personal data and sensitive data in the paper, but some things are sensitive even in public data. Public data: you don't want your name to be in public records. When you're looking into those it's important that classification of data is done. Is FIR a public record? Can I monetize an FIR as a public record? It's important to look at various kinds of datasets, and not just personal data and sensitive data. You need all sorts of data, and you can build it on public data which is respecting privacy. The distinction needs to be made based on what types of datasets are public. When you're talking about exceptions, you're talking about them in sectors, like for journalists. Data needs to be minimised in a public record, but it can't be minimised in terms of purpose limitation.

You haven't looked at the ownership of data. The paper doesn't do any justice to that. There's also the section on right to data portability. It recommends that machine readable formats for data. What we need is data standards. The paper doesn't talk about encryption. If you're talking about data protection, where unsecure channels are being used, that is not viable if you're not talking about encryption when you're talking about data protection. Without encryption, surveillance by state and non state actors is possible.

1358hrs: Roshan Agarwal: These things started with Aadhaar. India is supposed to be an IT superpower. However it gets a fraction of the revenue. Regulate only what is needed. Stick to Aadhaar. Also should have had this paper in two languages.

1349hrs: Kiran Jonnalagadda: I want to look at a few things said. One is data minimisation. People are aware that data minimisation is good for them. One example is VPN, which comes with no data collection. People are choosing to use VPNs because they don't trust their internet connection.

Secondly, on data anonymisation. People say that anonymised data is safe to share, but it is not because it still shows statistical patterns. Apple has been experimenting with differential privacy and there are challenges. You need regulation on top of good technology.

When you do credit card payments, you have 2FA. The point is that the website that you do it on, it doesn't see your OTP. When you do it inside the app, if it reads the OTP and adds it to the app, it compromises the 2FA. There is simply no protection afforded. The Aadhaar app has time based OTP, but it issues the OTP secret through an insecure channel. Any good TOTP implementation doesn't happen over the air. Technology companies work their way around but operate on a good-faith basis. Regulation should take that a little more seriously.

There has been a statement made that consent is broken, and we should do away with it. This is a fallacy. Software licensing is complicated, and between developers the most promising things that came out was the open source movement. Which was about formalising the licensing for software between developers. There's an open source repository OSI, which maintains a repository of licenses. Another example is 15 years ago an idea of licensing for content was in creative commons. It has a simple explanation, and the summary should be good enough. This is how consent should be done. Can there be a standard short code backed by a document that you can trust. That's how you restore consent.

1345hrs: Good to see that the data protection law, as per the paper will apply to government as well. [missed the second point]. Apart from consent, which should continue hopefully, the other five basis in the white paper are reasonable and are worth adopting. We should also differentiate between the data controller and data processor. Lastly we should look at creating positive incentives for data controllers. For example, in certain jurisdictions there is an exception regarding data breach notice to data subjects. They have an onus to report it to the data regulator, not the data subjects.

There was regulation that created 2FA which was on a web browser. The browser enforces boundaries between websites. On a mobile the boundary doesn't exist. One thing that Google has started doing is that it's offering a VPN for free, along with Google Fi. Operating system makers have started the importance of VPN. iOS also now allows VPNs. Platforms have started understanding that VPNs are important for users.

1243hrs: Ramajit Singh Chima, Access Now: Anyone who tells you that a global framework doesn't drive what product managers do is lying. The GDPR has forced people to engage with this topic, and the number of studies commissioned

to discredit it shows how impactful it is. There is a set of global principles on privacy.

Do's and donts: [We'll add this later after checking with Raman. He speaks very fast]

Puttaswamy judgment has focused on people and not data. Learn the lessons from the TRAI on regulatory powers. Tries conducts a consultation for everything it does. If there is a privacy commission, it should be for creation for regulation, not enforcement.

There is a problem about data being misused.

TrustID allows people to create profiles of people based on aadhaar information. Innovation is important but some forms of innovation are not acceptable. There are examples even in AI where there are forms of activity that are not allowed. Deep Mind was fined.

1239hrs: Ashutosh, ASSOCHAM: We are at the cusp of a position where we can be seen as the leaders of becoming the data analysts to the world. India today has all the three types of economies: really advanced, developing and the underserved. If we can innovate and create for these three, then we can innovate for the rest of the world. WE need a regime that builds trust in our country, we will create jobs, income. There shouldn't be a regulator but an ombudsman. We're not just talking about the IT industry, and privacy will impact all industries so we need a common framework.

On data flow, law enforcement access and data security, the security of data in a cloud first environment, is not dependent on where the data is. There are checks and balances which are in place, and there needs to be an accountability framework. Data localisation and residency were not the first point and were later addressed, and we need to see how we can become the leaders in data analysis. there could be a gradation in terms of things like national security etc.

1232hrs: Debasish, Broadband India Forum: Any curbs on data will hurt the country more rather than benefit the country. What is data processing about? Who is it benefiting? India is talking about having a 3 trillion dollar digital economy by 2022. The point we're making is what is driving this digital economy, and thus any curbs on data collection and usage will harm the economy more. Who is it hurting if we could artificial curbs? let us not put ex ante curbs. If there are any noted harms that are evident then they should be regulation in place to make sure that those grievances are redressed, and the harms should have a redressal mechanism.

21st century is about IoT, cloud, M2M, big data, we believe India has the potential to leapfrog what has been done in the traditional IT industry. We can become the global knowledge hub, by undergoing rapid socioeconomic transformation fuelled by data innovation. Data is not restricted by boundaries. You cannot have India innovation and a china innovation. You need to have exchange of data. You need to be able to make innovation and utilise innovation

for public good. For data localisation, the IT industry would not have survived it. We should allow cross border data flows, and we recommend no restrictions on cross border data flows.

Regulation is good, but regulation for the sake of perceived harms and threats is not the right way to go. Give them the freedom but with broad overarching principles. Industry is conscious that if they harm the customer, and they work in a self regulated environment. Because they are all good responsible entities.

Companies are operating in an environment where they understand the implications of causing harm, so we suggest a framework about preventing harm, rather than providing restrictive principles of preventing harms.

1231hrs: Justice Srikrishna: should the law prescribe classification, or should this be delegated legislation? Should parliament look into it?

1229hrs: Ravi Gupta from NIC: Create classification for what kind of data can be provided or displayed prominently, and classify.

1228hrs: Justice Srikrishna: if constitution is not in 23 different languages, how will you prescribe by law that privacy policies should be in regional languages?

1223hrs: Arjun from SFLC.in: I wanted to address the point about notice and consent, and that we shouldn't do away with it. Notice and consent has not become obsolete. What has become obsolete is the legal form. It becomes a technicality. A number of steps can be taken to ensure that it is procured in a meaningful manner, by having privacy policies in a simpler manner. For this purpose, this should come with minimum standard disclosures, and disclose things that should be collected, what will it be used for, how long it will be retained, and how can you revoke consent. All of these information displayed by default then this will help in a big way to ensure that the consent is meaningful. In the context of the Indian situation, it becomes a problem for people to understand what these policies say, so using regional languages would help.

1220hrs: Rahul Sharma: If we form a law which becomes a non starter for startups, it will have an impact on our economy. We need to be careful about direct and indirect impact on the economy. India's outsourcing business have grown because of cross border data flows. We have to assess our situation. We don't have to consider EU GDPR as a gold standard. They've had discussions for 10 years. The final draft of 2016 is very different what the law for 2012 was. We need to look at how they started. The EU GDPR is more of a handle for imposing penalties on google and facebook.

[I spoke for a bit, pushing for data minimisation and purpose limitation, and addressed a few questions from Justice Srikrishna]

1207 hrs: Usha Ramanathan: I think a basic principle in data protection is that it is not about protecting data but protecting people. That's the fundamental principle. I don't think we should go around US route, because that's giving us

innovation but its also giving us monster. It's also important that a lot of what we're talking about data out, or resources.

I found the white paper disappointing because it didn't seemto be taking into account the problems and situation, and changing in the constitutional understanding of what people are. People have said that privacy and law should should wait until innovation is over, and should not impl

1204hrs: Kamlesh Bajaj, individual capacity: On data minimisation: the question on data collection is that should it be restricted in the first instance. The key point is that if we restrict data in the beginning, what are we achieving, we're talking in the context of innovation. The key point is on preventing misuse and harm. To my mind, data minimisation has the potential of harming innovation in the country. We've just started with AI, IoT, and if we put a condition which will harm innovation in the country, startups which need data, or innovation on drones, traffic control, we dont know which way this will go.

On adequacy test on EU GDPR, it doesnt serve any purpose. We've always treated this as a non tariff barrier. it doesnt increase or enhance security or privacy.

1230hrs: [Someone]: we need to incentivise data localisation not force it. We're living in the era of virtualisation, we will lose business if there is localisation.

TRAI has gone the MLATS path for law enforcement considerations.

11:59pm: Venkatesh from DSA: If we accept the accountability principles in our framework, we can... [sorry couldn't get his point]

11.59pm: Arghya Sengupta: On legitimate interest, do you think that this is a balancing test that we can leave to every single data controller in India?

11.48pm: Venkatesh from DSA: DSA urges that outside of consent there are other legal basis for processing data, including contractual obligations, compliance with legal obligations. To go into one extra level of detail, the question of what constitutes legitimate interest, and when you're taking about data controllers taking onus of the data they're taking. Whether legitimate interest constitutes intervening in individual rights. That's one part that I wanted to mention, that there are other legal grounds for processing.

The white paper points towards click fatigue. We believe implied consent could come in to relief some of this burden. this could be an area where the framework could focus on. For example, when you go through a turnstile at a metro station, you're giving consent. Wrt childrens consent, the age that we're proposing is 13, which is lower than GDPR and complies with US.

Consistent with our views of consent, we should have context for data processing when it comes to notice. Notice should support choices that are contextual. The number of devices that we use to access the same apps are increasing, and it could be complicated if we're looking at click fatigue based consent. One

suggestion could be outside of having consent int he device as well. Where you have a public place where you put the notice, outside of the device.

On data scorecard and consent dashboard, some of those frameworks have not been understood well enough. We caution against a consent dashboard. The reason being that as you see technology increase, and prescription could prove unworthy of the decision that you took.

11.38 pm: Amber Sinha, CIS:

We require a strong data protection authority, market incentives for data controllers to comply, vigilant and active citizenry and security enhancing technologies.

On consent, points have been made about consent fatigue. The puttaswamy judgment places informed consent at the centre of any data protection regulation. It would be unwise to hedge our bets only on informed consent. We need practices which would be termed paternal, but they're required for protection of citizens. We will empower the data subject, and he is expected exercise rational choice, but there is information o indicate that that doesn't happen. If we recognise that privacy is a social good, and we hold data minimisation dear, then entirely relying on notice and consent is not absolute. Especially when it comes to sensitive personal data, a risk and harms approach on top of notice and consent would be important. The nature of the consent needs to be clearly set out. The consent has to be freely given, informed and unambiguous. It has to be given as an express and affirmative act. Consent should not be a tool for coercion. When someone is being denied access to service because you don't want to give access to incidental data, we need to check if we rely on market forces. If the legislation sets out a clearly set of rights, that would be helpful.

On data localisation, I agree with what Apar and (karthik from Nishit Desai) said. Data vocalises also has various shaded. One form is that we mandate it exists in our jurisdiction, it would be exported but with a copy, and also where it can be exported without a copy. It's important that it travels with the same protections when it goes outside India. We would look at adequacy and safe harbour mechanisms.

Finally, I would like to make the point that what the white paper does not delve into in sufficient detail is surveillance practices, and grounds for surveillance. Given the kind of technology given to us, and the PUCL judgment, it should be important to check how surveillance can be regulated, and also regulation of surveillance will require the state to document its own surveillance practices. These are issues which require urgent attention.

11.36 pm: Justice Srikrishna: If you're doing business in 20 countries, can you say that you will not comply with the laws of that country? maybe some day there will be a global concept, but to start with, your suggestion seems to be that all localisation is wrt govt data, and wrt private data, there should be cross border flow without restriction unless there are security issues.

There is a link between consent and purpose limitation. In some cases even when consent is provided, and if there is evidence to suggest that it can't be acted upon in public interest. Consent should not be an immunity from liability.

11.33 pm: Pankaj Sharma, Telenor: as telecom industry, we've faced this quite a lot. This has been one of the first hurdles. The current rules are, and led by security agencies, are about data localisation. That you can't monitor something outside our borders. The reason for issuing these issues is that there is no global framework for data and privacy. We need to move in that particular direction. How can any country apply a law that is not applicable in their country.

The moment you say the server has to be in India, the global aspects of efficiency will go away.

11.32 pm: Shruti Rao from Information Industry Technology Council: We'd like to opt for a globally interoperable regime. There need to be global voluntary standards. We emphasise that there should be no data localisation

11.30 pm: Kartik Maheshwari: on data localisation, when there are arguments for stored in India, the criteria for empanelment for Meghraj, the govt data is being stored in India. The interests of data subjects and industry are exclusive.

11.27 pm: Smriti Parasheera, NIPFP: data protection is also about your day to day dealings with your employer and university, and not just big data. The calls for abandoning consent shouldn't be there. There are really contexts where consent can work quite effectively. For people who say there is consent fatigue: yes there is, and it has become difficult. Just as tech has made consent difficult, it also holds the solution for it. Then the idea of privacy by design needs to be talked about. There is no one size fits all, and we need a graded approach. The role of data protection agency and agency design is important.

There should be a principles levels approach at the level of a primary law, and have a strong enforcement framework for all of this.

11.24pm: Apar Gupta: The committee in the white paper has noted the work of professor Anupam Chander, his basic rationale against data localisation is that user interest and business are not fully satisfied and give governments more censorship control, and create barriers for business and users from availing services. Countries which have harsh data localisation laws are China and Russia. His work argues against it. I would argue against data localisation. There are several rationales for user interests. For business interests, a large part of the data localisation push comes from Indian industry, which wants to erect competitive barriers.

11.20pm: Shagufta Kamran: Internationally, there are frameworks like OECD which provide good guidance around cross border data flows, and harmonising with them would be useful. Too much prescription will not go in the favour of the industry. Self regulation should be the regime. If we encourage data localisation, it will be disastrous in case of natural calamities. Allow cross border data flows. In terms of the multiplicity of actors involved: there are a lot

of allied laws. The point is how far are we incorporating the necessary changes in those laws as well.

Data as a concept, or a basic principle applies to various sectors. We need to start engaging with the automobile sector and other sectors, who are in possession of that data. There needs to be a distinction made between data processors and data controllers. That's best governed by contractual laws.

11.18pm: Pavan Goel, individual: The public conversation has been around Aadhaar, but there is private data owned by google and facebook, and this data is stored in the United States. The US laws provide privacy guarantees only to US citizens. These services either willingly or under a US court order violate Indian citizens privacy. Our law may be against that but it will be in conformance with the country where it is. One solution: it's necessary for this entity to have an Indian entity. In order to reconcile jurisdictional issues we should have data in India, and only allow cross border data flows which allow data access.

11.12pm: Pankaj Sharma, Telenor: The team who wrote the paper needs to be commended. What we need to understand here is that as India, we are the cusp of a digital economy. We are looking at questions which are really framed with the right intent, we could have a good regulation, but we could have a disaster for digital India. We should discuss this question by question.

On notices and consent is that consent fatigue is already there. I don't think anyone reads it, whether us or anyone else. What happens is that the aspect of having the facility is taken more than privacy. We say yes to everything. What are we going to incorporate which is going to matter. We need a simple law with protection, and the notice says as long as whatever is happening is being covered by the data privacy law of India, it should be okay. We can't have lengthy consent. If you're talking about privacy law, the paper says that there are two types of data which can be used: anonymised and pseudonimised. Then consent part does down. When do I need to share my data? Or the portability of data. These issues come when I'm interested in sharing that data. As a data controller I want to use the data or as a consumer I want to share my data. If they can use anonymised and pseudonimised data, no consent is required. For medical records, we can have a stricter law. Even for Aadhaar there is an OTP based system. I could say okay on biometric based system.

For Children, it has to be over parental guidance, and that age could be just 15 years.

1110pm: Charu Malhotra Indian institute of public administration: This is less about data and more about people. Data protection has two aspects: the privacy issue and second is commercial issues. I did not find clarity on the remedial action in case it is breaches, in case a company breaches data protection for the masses. Let citizens be partners in crime in case of commercial aspects of data. Why aren't we able to think of a dashboard scenario, if I give informed consent

then I know where data is given in the pipeline, and what is my percentage share of it.

1109: Sharad from institute of company secretaries: About medical records, it's sensitive information for patients but important for regulating the medical profession. How to balance this, because the data has to be provided for competition, but sensitive parts could be taken care but also competition is taken care. Balance has to be maintained, it should be portable, available for research as well.

1105: Ujjwal Kumar from CUTS International: Data protection isn't just necessary from data protection, but also from competition point of view. The right to data portability is something I want to flag as an issue. Every economy follows its own rules and philosophy. Data portability needs to be upfront as a principle, because it goes beyond privacy. The right to data portability depends on the definition of personal data. The larger principles should also include the consumer usage data, allowing them to be portable to help increase competition.

1103: Gopalakrishnan S: Topics for discussion:

- How can notice and choice be incorporated in a data protection law to operationalize consent? How can children's personal data be effectively protected?
- How should "data localisation" and "cross border transfer of data" be dealt with under a data protection law?
- What should be the nature and scope of the possible exemptions under a data protection law in the Indian context?
- What are the different types of individual rights, their nature and scope which can be incorporated in a data protection law?
- To what extent should data controllers be held accountable under a data protection legal regime?
- What will be the impact of a data protection law on allied laws, particularly, the Information Technology Act, 2000, Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, and Right to Information Act, 2005?

1101: Justice Srikrishna: We're here to ensure that the data protection law, which has been the buzz word in the country, becomes crystallised, and the inputs that are necessary to crystallise it are taken forward. An opportunity has to be given to stakeholders what their concerns are so that they can be noted and addressed.

If you point out a flaw, I'll say what is your solution to your problem. I want solutions from you. We'll note what is wrong, and set it right.

Notes from Srikrishna Committee open house in Mumbai

We tried to liveblog the data protection committee consultation in Mumbai yesterday, but Internet connectivity at IIT Bombay was pretty poor. Below are the comments that we were able to note down: these may somewhat paraphrased, often exact, but shouldn't be treated as a verbatim transcript. We missed some bits, and skipped some comments, which we either didn't get, or were repetitive, or when I was commenting. We've identified speakers wherever possible.

Also, I reached some 15 minutes late, so only caught a part of some great opening remarks from Dr Anupam Saraph, which haven't been included below. Two fun parts: firstly, a person from Hindustan Unilever saying that he's speaking in his personal capacity, and then going on to make a company specific comment. Secondly, an ICICI Bank representative trying to justify buying personal data from clubs etc and using that for marketing (i.e. spamming). Go figure. Anyway, here are the notes from yesterday:

Update: Anupam Saraph send us an email with the points he had made, which he shared with Justice Srikrishna as a letter. Here's a summary:

Is data protection technology centric?

Data protection cannot be the protection of data in a particular medium like digital. We cannot create a data divide by restricting to the digital. We cannot borrow technology ideas either. For example eKYC is not KYC. KYC is not reusable as eKYC is. There is no identification in authentication. We are creating a legal mess by using authentication where identification should have happened and we assume it has happened by authenticating biometrics. We cannot automate business process without preserving original responsibilities. For example the branch manager used to be liable for account opening and creation. Now no one is.

Who is the beneficiary of data protection? Who do we protect and from whom?

The people whose affairs generate the data when they engage in a, legal, common purpose must be the beneficiaries of a data protection framework. For instance the banker and customer come together for a common purpose. Similarly the citizen and the PDS come together for a common purpose.

The beneficiaries *cannot* be third parties who seek profit from data of systems they have no role in, share no common purpose with the parties whose affairs generated it, and do not have any skin in the game to protect the parties whose activities generated it. For example, the data of the banks and their customer or the citizen and

the PDS are not generated for third parties who have no role or skin in the game to further the common purposes of those in the system.

If we fail to keep away third parties, they will colonize, corrupt or destroy those systems whose activities resulted in the data.

For instance: Neither the UIDAI nor its “ecosystem” have any role in the affairs of the people who have come together in different systems to further their common purposes—from enabling borrowing and lending money, enabling ability to connect and communicate with others, obtaining education, ensuring ability to travel abroad, to ensuring food security, or even to get a dignified burial. UIDAI has no understanding or role in the common purposes nor does it protect or further the common purposes. It has no skin in the game. This overreach destroys the symbiosis between the borrower and lender, the mobile user and service provider, the passport issuer and traveller, the hungry and the food provider. Along with the UIDAI, the GSTN and the NPCI, for example, are similar third parties that seek to profit from data of systems in which they do not share any common purpose with the participants of the system. All of these demonstrate how third parties have colonized, corrupted and are destroying systems that worked well before the intervention of the third parties.

What is the purpose of data protection?

In end analysis data must be protected because it furthers the affairs of the people whose affairs generated it; it is protected to ensure their affairs are just, free of inequality, free of indignity and do not destroy their liberty. After all furthering the promise of the Preamble to the Indian Constitution is fundamental in governance.

What should be the scope of data protection?

There is nothing more important to those in any system other than empowering their common purposes. In the process of pursuing the activities towards the common purpose in any system, data is generated, certified, authenticated, updated and also restricted from use by third parties. It is also audited to increase confidence in the protection of the data throughout its life cycle.

For example the delivery of rations the generation of data, its certification, authentication, updation and restriction cannot be unequally or unfairly regulated by one participant or an outsourced agency without skin in the game to serve the purpose of ensuring no person is denied rations on first visit.

The scope of data protection framework cannot, therefore, restrict itself to privacy or restriction of data access. Privacy does not protect the parties engaged in common purposes unless the entire data life

cycle is dealt with. In fact data restriction is not just about privacy but also about data sharing.

Furthermore a data protection framework cannot restrict itself to digital and create a data divide. Any data protection framework should as much protect the non-digital as the digital. The Constitution is not about the digital or data economy, it is after all about ensuring justice, equality, liberty and dignity.

What are the principles of data protection?

Data Protection framework needs to protect Indians to ensure at least minimum protections. Here is just an indicative list of the protections that the Framework will need to ensure.

- Protection principles have to be based on the objective to ensure justice, dignity, equality and liberty of those whose engaging in common purposes results in the data that is required for the functioning of their systems.
- Protection must ensure that the protection of databases that protect the sovereign, democratic and republic status of the country.
- Protection must include the protection of the manner of creating the data, certifying it, authenticating its copy, restricting its use, auditing its creation, certification, restriction, updation as well as ensuring its fidelity and updating it.
- Protection from coercion of any party to need to participate in any scheme in order to create, obtain or use data, that forces digital, includes parties without any skin in the common purpose of the system generating the data, exceeds in scope, or is contrary to the common purpose of the system they participate in.

The Economic Times recently ran the story of all of India's Electoral Roll with 68 attributes of each voter for every constituency being offered for a price by an American company. This indicates that there is no way the Election Commission of India, or the voters will be able to distinguish between the real and a fake copy of the Electoral Rolls. This is a failure of the four protections listed here.

The use of unknown database to open 37 lakh bank accounts and transfer 167 crore LPG subsidies into them is another example. Another is the metering of broadband by ISPs to throttle speed or block content in violation of TRAI regulations and NET Neutrality.

What are obligations of parties who generate data while engaging in their common purposes?

It is necessary to develop a minimum set of binding obligations for transacting parties generating data so that this data can allow them,

or any neutral arbitrator in case of dispute, to be able protect the justice, equality, liberty and dignity of the participants in that system.

- Those who participate in the transactions of a system have an obligation to ensure sufficient data to protect justice, dignity, equality and liberty of all participants.
- Data may not be outsourced to data analysts to become entrepreneurs or build a digital economy off the data of the affairs of others.
- Parties, from within the transacting parties, responsible for keeping a repository of the data should document the agreed policies on creating the data, certifying it, authenticating its copy, restricting its use, auditing its creation, certification, restriction, updation as well as ensuring its fidelity and updating it.
- Any breach of data, at any time in its life-cycle, will be reported to all other parties of who have come together for common purposes. They should jointly assess and report the damages to their common purposes as a consequence of the breach to the law enforcement machinery for investigation and prosecution.
- Any disputes about data protection should be referred for arbitration under the Arbitration Act with machinery that can satisfy the requirement for interim relief within 48 hours in the matters of life and death.

I handed over a copy of this in the form of a letter to Justice Srikrishna.

Speaker: The adjudication mechanism is not working. It often leads to compensation and damages.

Justice Srikrishna: What kind of mechanism are you suggesting?

Speaker: Why don't we have an online dispute mechanism, where the judiciary interferes at the end. The organisation or the regulator works this online dispute resolution. The redressal handling mechanism of digital india has failed.

Everything seems to be linked to consent. It's based on one single button which has I agree. There is no statutory mechanism which legalises I agree. It's dicey: how do we take it as evidence when I agree button is pressed. Is one sided contracts legal? **Lets legalise via the *I Agree* button where there is some statutory support.** Consent is going to be based on one button.

Deliberations have been going on related to a [Privacy law]since 2006. Aadhaar has been fining people when they keep data at a local level. You put an FIR on them, but what happens to that data? Huge amount of data is with them. Can't we have a right to purge? Courts will have better decision making power.

Justice Srikrishna: We are so focused on digital transactions, we forget what

is going on in digital life. That is required to be statutorily there for a specified period. Can we say that it should be immediately deleted or permanently deleted.

Speaker: What statutes are mandated, what is the amount of time that the data is withheld? Should be between 3-5 years, and other reasonable restriction in courts, till the matter is not settled.

Malavika Raghavan: Data risk is one instance that we're interested in. The key question is, what is actually personal data. Our proposition is that it should be personally identifiable information. We don't think there should be a distinction between sensitive personal data and personal data. We will end up landing up where we are now, with a meaningless list approach. The fact with big data is that proxies are used as links to information. The first proposition is that we should have one standard of personally identifiable information, and there is no excessive compliance issues there.

On NTPs: there needs to be a difference between controller and processor. If you can slice up the controllers into systemically important entities, medium risk entities and low risk entities, and engage with them to prevent data breach. Pre-breach, what non threatening measures can we take. Can we give information guidance, and talk about private warnings, public statements before you have the mass scale breaches before there is panic. On the point of consent, whether it should be a primary ground of processing: it should not be a primary ground. It should exist, but the role of consent has changed: it is a notice to the individual, and no longer is it a permission. All the obligations there should be a legitimate purpose test. There is a six clause formulation: whether the collection is legal, necessary and proportionate. So you balance the interest. Consent is no longer what you look to understand the right and the obligation, whether it is necessary or proportionate. If at any stage it fails the test, of collection, processing etc.

We've spoken with multiple providers who are seeing data as risk, and see it [data] as a toxic asset. Co-regulation is an important tool but it should be a part of the responsive framework. There can be a pyramid of sanctions, and a pyramid of support, for better data practices. One is the point of protecting individuals. Secondly it's important to enable data flow.

Rama Vedashree, DSCI: What is the framework that you have in mind to classify controllers as low risk, medium risk and systematically important?

Malavika Raghavan: The finance sector has some points: if you look at the Basil committee, one part of it is interconnectedness. A central database which a lot of databases use. Another is the volumes that they are exposed to. There are issues related to capitalisation. What is relevant is the amount of people's information they are holding. When you categorise, organisations should have enhanced supervision tools. There are other tools that they could have. A lot of larger organisations are open to regulatory conversations. This can help reduce and minimise the risk.

Justice Srikrishna: Instead of being systemically important, it could be important from the point of view of the harm it could cause.

Malavika Raghavan: If you have at a market level the electoral rolls being called into question, that is different from inaccurate info for a few people.

Vikram Gopikar, TCS: My question is specific to article 2.3, which calls for retrospective application, whether that would be feasible. There is an illustration in the South African regulation, within one year of collection, they need to be applicable to the act.

Justice Srikrishna: Data is already collected. All the data collected is capable of being misused. Should it or not be subject to the same stringency as what is collected today? Deal with it the same manner as it is today.

Nancy Jane: There are laws missing: for example IT guidelines for cybercafe rules. Quite often we give this information, and the data is both digital and non digital as well. Both the non digital data should be protected. DSCI had come with a manual. When the police collects data, in case the data is leaked it affects the image of the victim. There are times where rape victim videos have been leaked. Related to corporate espionage, should juristic persons be protected? they should be. Considering that there are lot of infringement, we should protect their interest as well. There is a responsibility to protect that as well. Data protection should be retrospectively applicable. There should be a time-frame given for compliance.

Aditya Birla group representative: A lot of data is going to be with the government and it should be the role model, and Aadhaar data is with the government. There are chances of leakage. It's important that we apply the principles as well. Another important point which the industry is facing is the extraterritorial jurisdiction. If we could have a treaty at a country level for a safe harbour, it would help us.

Justice Srikrishna: What are you suggesting when you're talking about extraterritorial jurisdiction? Is it data pertaining to India, or to Indian citizens?

Aditya Birla Group: If it's an Indian citizen, there should make the person accountable if they're extracting the data. Thereby the citizen of India is feeling secure. From a GDPR perspective, the way the law is, that they have extraterritorial jurisdiction. Somewhere a treaty as a global level.

Justice Srikrishna: That is a matter of international treaties, and not of the law.

Aditya Birla Group representative: I don't agree with the principle of localisation of data, but certain sensitive data can be localised.

Ashwin, VC: Related to anonymised data: it's practically impossible to use anonymized data, and ensure that it cannot be used beyond the scope. Anonymised data should be defined which should be out of the purview of private data. That is needed because many laws and frameworks cannot be

implemented on certain data, in terms of scope. It's practically impossible to define the use and inform the user.

Krishna: We should stress on privacy and data protection of India, instead of data protection act. We need to stress on it, and keep on repeating privacy, privacy privacy. We need to consider social cultural aspects of India, we have specific sensitive elements. When we define the personal information and sensitive personal information we need to look at social aspects. Consent is coming ahead of notice in the draft, ahead of consent. Notice needs to be ahead of consent.

Anveshan Roy: We work in understanding movement of people in and out of locations using wifi analytics. Our recommendation of MAC ID should be non personal. Every device has a MAC ID, and that is not personal information. Seeing the potential in India. One cannot identify the person by the MAC ID.

J Srikrishna: How is it not personal?

Anveshan Roy: If you have a wifi router and a sensor, your phone has MAC ID should not be personal if it is anonymised completely.

Gulshan Rai: Technically it is possible to identify the MAC address of the person.

Anveshan Roy: If I'm the only personal in this room, I can do the reverse engineering. MAC ID has to be tagged with other form of data capture. For us, the initial bit is anonymised and aggregated. We're not capturing IP address.

Anveshan Roy's Colleague: MAC ID is not identified. If it is merged with another data sourced, consent should be required.

Another speaker: IP Address should be under the personally identified information. Each category in sensitive personal information should be very well defined. Regarding the children, in cybercrime, most cases are children related. The pictures should be asked only if necessary. People take pictures, upload it. If it's a 16-17 year old, the pictures are going into the dark web. We need to take care. Take it only when necessary. They should give them an option, even when the school is storing this information in its database, we need protection of data and enforce certain rules. The concern is of privacy of children. The last point is: even parents, are posting pictures of children. Some warning systems for information like that.

Malavika Raghavan: On the horizontal application point, it would be meaningless to have different laws. The interesting one is around jurisdiction: one is the territorial jurisdiction, it should be everyone in the country. no provider can check your citizenship. There are companies who are conducting business in India, anyone buying goods and services should be protected irrespective of where it is being delivered from. Where there is an entity outside of india, and there's a process, even there, where that processor is processing data in India, there should be a cause of action against them.

Identifiability and anonymisation: it must be a technology neutral law. The questions will be specific: the first is related to the identifiability of the individ-

ual. The law applies to an identifiable natural person, and this can be defined. You can provide a list which is indiciative list at a principles level. Anonymation and pseudonimisation technologies are evolving, if its not identifiable then its not applicable. We can come at clear articulation.

Justice Srikrishna: if it's not applicable today and is possible later, the law should apply later.

Gulshan Rai: How do you classify rights on entities outside of India?

Malavika Raghavan: The first is the jurisdiction clause: Foreign companies doing business in India, second is whether they are data controller or processor for our purposes. The offering of goods and services, you would have a claim under the consumer protection law. Purely on the fact that they're offering goods and services. There is a legitimate purpose test....

Gulshan Rai: He's a data collector when you open the account. The other is when they are storing the data.

Malavika Raghavan: the third aspect is legitimate purpose. We will need sector specific regulations.

Anupam Saraph: A concern: increasingly there is a trend that harvesting of information is normal and natural. It assumes that there is nothing wrong about it. If we have to protect somebody, and protecting people who are transacting parties The minute we forget that, where I can photograph and bug you throughout the data, or access to your bank account that I have the right to harvest for whatever purpose, is completely irrelevant. There is no wilful consent and participation. There is no legitimate reason for collecting this. I think this as a big concern. Who are we protecting and whom are we protecting them from. If we don't define these two parties, then we would have lost an opportunity to say that data isn't the new oil. it's not another commodity, It's about ensuring that by protecting data we can build transactions of parties within the country.

Justice Srikrishna: That's where malavika's formulation about consent. There is accident and evidence. The purposiveness of the test becomes important. The purpose for which security camera will get a tick mark.

A speaker: The lessons from the IT Act have to be implemented. The implementation lacks the teeth. The second is the awareness to the data subjects. Are we making some efforts to tell them what is privacy.

ICICI Bank representative: On purpose specification and a citizens choice...One citizen might not want to get offers given to them which is not directly related to what they have given consent to. There would be others who would want this information. A choice to the citizens should still be kept, and citizens should be given an option to opt. There's massive criticism on clickwraps, unless people agree to the terms and conditions. If we want to give someone an option, should the law prescribe what should be informed consent?

The person may not choose to get the information, but the service should still be available.

Notices which are to be given, the paper talks about consent fatigue. From an industry perspective there could be a common notice, which could be framed with the sectoral regulator. Every bank is going to send a similar notice.

Often there is a requirement to source customers. Once a customer comes and engages with an organisation, it is only then they enter into a contract. When you are trying to source customers, like in club diaries and industry manuals. How should that organisation be liable for using that data which is in the public domain?

Justice Srikrishna: If I become a member of the club. I give them my data. I give for the purpose for my association with the club can be carried forward. If you as ICICI go and take it, isn't it a failure of the purpose test? I didn't allow the club to give it to ICICI or HDFC? How you source your data, you find out what can be done. But today I get emails from ICICI.

ICICI Bank: There's a distinction between sensitive personal information and personal information. How we were perceiving that was in terms of the harm which is caused. In the prospective list, under the SPDI rules, it includes financial information. While all other constituents, which is intrinsic to a human body, the harm which can be caused with that data is different from financial data.

Justice Srikrishna: Financial data is personal data. Tomorrow someone finds out you have Rs 100 crores in the bank and you'll get a call from Dubai. Sensitiveness to data is apart from the inherent nature of the data. It is sensitive.

Gulshan Rai: Malavika was saying that you raise the standard of personal data [to sensitive personal data, and not that you reduce the standard of sensitive personal data to personal data].

Professor Nagarjuna from TIFR: The law should have a directional principle, where you would say what kind of measures would enhance data security. There is a linkage of information to a large number of agencies. One clear law that one can make is to say that the greater the linkage, the greater will be the leakage. If you have 1 billion people, each person has at least 10 social service leakages, there will be 10 billion leakages. Therefore, is it in the scope of this document to specify what kind of measures would enhance data security? Could it say that linkages to various services should be reduced. There may be business interests, and other interests, but not in the interest of citizens. Greater the harvesting rights given to people, the security will come down. What are the models that will decrease or increase the data security. We are talking about data processing techniques. We need a public audit of data processing. Similar is the case of encryption, rather than some expert committee, because there is a possibility of selection of experts. It's also important for us to say that when I give consent, the agency should also give an undertaking. There are devices that

we use which have device identities. They are potentially capable of becoming sources of harvesting.

Justice Srikrishna: You're saying that there should be an undertaking. Why is it needed if the law says you're liable. Undertaking is what he tells you as private contract.

Prof Nagarjuna, TIFR: Doctors give an oath. Those are some kinds of roles and responsibilities.

Justice Srikrishna: (something on the lines of an oath is a moral commitment, and not enforceable).

Sandeep Arora, Market Research industry: One of the things that I've noticed, is that we seem to be too worried. We're seeing the dark side. In this world today that there is so much data that it can help people. We're able to understand the causes of diseases. We have the technology today, it would be foolish and myopic that we don't do it for the better benefit of the humankind. I would want to enhance the motivation of the law, that it has the necessary balance in place for us to ensure that the benefits that it brings to people and consumers is kept in mind. I have a couple of points: In market research industry, we need to keep understanding people. It can lead to a state called mass customisation. You can give a larger solution at an aggregator level, we can understand mass customised solution raise. We need to keep understanding a person more and more. If you have understood them once, you can go and ask questions all over again, or you can go to a proxy and start from thereafter. For us it is very important that we are able to maintain and get incremental insights.

On the quality checks: we have to go back and perform the necessary checks, and for that we have to maintain recontactability.

On informed consent: There are two-three elements. One is a blanket consent. Do I really, as a consumer, a right to negotiate different parts of what I'm consenting to. I have to go and agree. There are some dark elements sitting there...

Justice Srikrishna: When I go for a LIC they ask me hundred questions, and say I give you only my name and age? Therefore, the larger test would be purposive.

Sandeep Arora: Sometimes we are not able to understand the purpose.

Ranjeet Rane from Reserve Bank IT, speaking in personal capacity: I think that the law should take into consideration that in a very small span of time, we have seen concepts like password become irrelevant with technology. For example, fingerprints. On the financial information side, the law should list down what should list down what should be sensitive. Considering that we are aggressively pushing financial information, I would request the committee to have a view to look at financial information as sensitive personal information.

Beni Chugh, Dvara Research: Two issues keep recurring: for how long should the information be retained. If we think of legitimate processing test as a step

of the framework. It's more of a framework that we're proposing. The CICs are required to retain data for seven years. For other records like vaccination, these are taken care of by the legitimate processing test. There is a need for sectoral regulators to come. On consent, there is behavioral economics to show that it cannot be the exclusionary ground. On one hand, you have legitimate processing, and the obligation to not cause harm. We come at a solution that emerges organically. If I take a photo at a photo booth, it can't be sold on the dark web.

Shagupta USIS: In terms of the right to be forgotten, it does not allude to the context. To our mind the use should be very limited, in case of theft and financial fraud. It would be better to have broad principles. We saw TRAI and CCI getting into a conflict. The third part is data localisation: that there shouldn't be blanket localisation.

In terms of data processors and controllers, there are intermediaries. They might not be processing or controlling the data.

(made some more points but spoke too fast)

Data minimisation should be replaced with a no harm principle, with artificial intelligence coming in.

The penalties should be in proportion to the harm. Just because the companies have high turnover....

Wrt children, we feel that there could be 3 categories, where it is less than 13 years, where parental guidance is mandatory. Next is 13-18 with individual consent along with parental guidance, and then above 18.

Vickram Krishna: Much of what is concerned with communications impinges on the personal sphere. We are close to a cusp where we are in a position to be a serious global player again, provided we have the right laws. One thing that is critical data management. If there is some place in the world where it is very very important for how personal data is handled, that is a model that we have to respect. If you look at Germany, one of their largest auto makers, Volkswagen cut a sorry figure where they were trying to defeat global standards. What's worse is that Germany has taken a hit for the understanding of technology. We should be setting an example to the world for how we can respect the personal data of our citizens at a level that is at least as high. This is really an opportunity for us and we must take it.

Suvendra Tulsian: It looks like everyone is overcautious about data. Law should be practical, but we cannot ignore the technology. Law which is good for Europe is not necessarily good for India. Most of the discussion is about protecting data at storage or in transition. Look at the way data is generated: Whatever data we have with UIDAI is protected. Can the UIDAI guarantee that the fingerprint they're getting is not getting leaked? If the whole purpose of UIDAI is properly authenticating the user, they cannot guarantee authentication, how can they allow financial transaction using Aadhaar. One is the consuming party and

other is verifying party. The law should make both parties liable for ensuring that the right fingerprint is submitted. The third suggestion is about MAC ID, that one should be able to capture it. In IOS and Android MAC ID is not allowed, because they understand that this is a problem. Because directly and indirectly one can reach the person. We need to recognise the machine but it should be using a virtual ID, not MAC ID. The only use is on the organisational side. What the device is the company shouldn't come to know.

Harsha Vohra, Data Locus: In the previous law there were definitions of data and access which were broad. We had to take legal opinions from multiple law firms, and not even two of the opinions were same. At the same time, companies in western countries they could formalise a code of conduct. My request is to a data protection authority which could be used by entrepreneurs to take a decision before they start up. We've seen that a lot of innovation is not happening because the laws are not clear. Companies in the US which work on images captured by satellites. Laws can be formed to help in these kind of innovations.

Shreyas Bhargave, Capgemini (personal capacity): The need for physical documents as proof when we're doing eKYC. If we talk about data security on the digital and physical side. Can the law specify remove the need for physical documents if we're doing in a digital manner.

Justice Srikrishna: People collect for purpose. Data minimisation is the principle.

Speaker: gives example of new android guidelines, and says that there should be function driven purpose limitation.

Justrice Srikrishna: That is what Malavika (Raghavan) was talking about with purpose driven regulation

(Someone sitting in front of me turns around and says to Malavika: This will be called Malavika's Data Protection Act :))

NS Napinay: I was under the impression that the consultation was going through follow through in the question format. I have a lot more questions than answers. We are faced with a situation where dolls and toys are collecting data, TV shows are facial data, not just usage behaviour. Whether it is offline or online, we don have ring fences protecting information. India has the advantage of doing cherrypicking. The white paper has a west to east flow, in terms of laws. We are on one hand are looking at taking from robust regimes who have learnt from their mistakes, and we are looking at jumping on the bandwagon and going to the gdpr. How ready are we? How much confidence can we have of data controller with just conformance rather than compliance. We've had some skeleton laws in the part of the IT Act. They prescribe certain provisions. Every single provision has been treated more as a tick mark. We may even have a due diligence. Each just leads to a report being filed and it doesn't reflect reality. 90% of what is laid down will result in compliance, but even in the compliance,

if we can ensure that merely the tick marks protects the individual rights, we would gain.

Justice Srikrishna: Vishakha guidelines have been in operation for so many years. Every company has to have a special committee to deal with sexual harassment. What implementation do you see on the shop floor? The law is good. The mindset has to change? Is there any solution?

NS Napinay: only two things drive the world: Fear or greed.

Justice Srikrishna: that is right, so we have fines on global turnover, or prison.

NS Napinay: the command and control and coregulation: Self regulation and coregulation have always worked better than command and control. Command and control only works only if we have a fear of retribution which results in its adherence. That's the way we might have to go with data protection: not just the kinds of data, but also balance the kinds of protections we are putting for each kinds of data. What is the purpose: to protect the individual, empower, enable them or just to enable governance? Is to enable businesses, whether big data analytics. One flip side of this is that businesses need as much leeway with data as they need a law. If we don't have as much of a robust law as the EU GDPR, so business comes here. It needs to enable rights and puts the individual at the centre. The governments rights have to be balanced based on the social contract theory that it is the individual that prevails. "And the law hangs limp, and barks but never bites". TDSAT cannot be an authority to decide on data protection, or cyber issues. The secretary ministry IT cannot be the adjudicating officer. When I look at the Schrems case, my utopian dream would be like the EU Court of Justice in India. If that isn't enabled, what will the act be about.

[Came in post lunch]

Rahul from HUL: Part of the data governance team, but speaking in personal capacity. For most of the ecommerce companies now coming, the natural method of the business means that they collect a lot of data. One big purpose is enhanced consumer experience. The other essential entity is the manufacturer, whose product is traveling back to the household. Manufacturer also wants to enhance the consumer experience. If there could be a check-button which allows the consumer to say that I want to give the data to the manufacturer.

There are many companies in the space of technology who are servicing consumers and businesses, and there's always a chance of interlinking data from one to the other, which gives them a magnitude of strength. There are entities like Google, which has its android platform which can be shared for their services too.

Debashish Bhattacharya from Broadband India Forum: There has been a lot of talk about why we need to protect data. Just to play the devils advocate, where data has not been used to harm anyone, to write the law in a manner that kills sources of innovation is not a good idea.

Today India is being looked at a global knowledge hub. We are undergoing innovation which is data driven. Data innovation and privacy can be compatible. The data driven innovation cannot be scaled without adequate privacy safeguards, without the trust of the users. Hence it is critical to empower users without overregulating. The law needs to be outcome driven rather than prescriptive.

Secondly, collection and processing of data should be allowed with minimal restrictions, where there should be control for the data subject, with the right to recall and opt out, and the accountability for the data controller. The next point is that preventing harm principle is a better approach. In terms of the comparison between the roles for the data controller and data processor. The law should not unreasonably intervene in the relationships between data controller and data processor.

In terms of a data protection authority, there should be corporate accountability and an ombudsman, the principle should be a self regulatory model. Only in case of a deviation, the ombudsman should have a right to intervene.

In terms of right to be forgotten, it should be for information not publicly available information.

IIT Mumbai professor: Oil produces production and should be taxed, and therefore when you're using someone's data, they need to give proof and why they're using it for. The onus on collecting the data is on the controller. There are now tools available, and philosophies like distributed computing, privacy by design. Things are possible. Why not have laws that are not enforceable? You could make references to these things to give direction. Data has two roles, like a knife: for murder or cutting vegetables. We are formulating new laws. Google and Facebook are very powerful. These are very powerful entities. If it fine to have a legal framework in which they manipulate and control us.

Ajit: On data localisation, I have a view that asking for data to be localised put a lot of problems from an economic perspective, but is there way to force service providers to give direct access on an MLATs process? If that can change then that is reasonable. Something which says that anyone who provides services in the countries, that would be good. We shouldn't be asking for data localisation. I don't see anything in the paper about information on dependent entities. What are the expectations from a privacy perspective?

Cognizant representative: We have captured things from a transactions perspective, and most clients say that India isn't adequate. They offload a lot of things on us in the clauses and there is no negotiation. The business team has to think about an Indian version of GDPR, with the same rigour. If the committee could take that into view, while drafting a bill. In terms of access to data by data subjects, when requested by data subjects, we need to give access and modify.

In terms of the DPO, it is a cost. If the law imposes such a requirement, it is a cost. Our submission is that please keep that flexible to not keep an in-house

DPO and outsource to an agency like a company secretary.

Puneet Awasthi, Market Research Industry: We collect personal data and opinions. If a person after a year of volunteering that information, and if a large number of people do that, then that has a huge impact. RTBF should be for personal identifiable data, and the analysis should remain. There's also under element, around defining elements that constitute private and personal data. There are data which are not identifiable with a biological entity.

Shivani Nadkarni: The law that comes out will create an ecosystem of auditors, DPOs etc, and one the biggest challenges is that the awareness is very very low. Very few people understand the difference between data privacy, data security and data protection. The awareness levels need to be increased. Some suggestions I had: There is a mention of bringing out a pictorial notice. What are the other ways in which consumers are in a position to understand and take a decision. Organisations could be helped with specific standards and guidelines in their form of seals and certification, which helps them understand the level of risk and compliance and thus take a decision. The law could build in structures to build these kind of implementation.

Ayushi Mishra: Is this law on the horizontal level or the vertical level?

Justice Srikrishna (with a twinkle in his eye): The law will be spherical in nature. It will cover all 360 degrees.

Naman from Access Now: [gives too long an intro about Access Now] There needs to be the withdrawal of consent, allowing the data to be deleted. The second would be regarding self regulatory mechanisms: in Europe and otherwise, only mandatory frameworks work and are required. Industry inputs in terms of what they should be and how they should evolve, and are required.

Brinda Mazumdar: The scope we're talking about in terms of natural persons, looking at both the living and the dead. Even dead persons personal information could be misused.

Justice Srikrishna: In Puttaswamy, no one argued for a dead persons Aadhaar number.

Ayush, from Bloomberg Quint, speaking in his personal capacity: There has been a mention about informed consent. The point I want to make is that people have concerns around the data that the big tech companies have. The first is that the monster in terms of what access they have, is a lot more nuanced. The kind of permissions that we're giving these apps. In the UK everyone talks about iOS giving more secure than android, while Google is facing a class action suit, where data was accessed by Google. Google's response is that they used a Safari workaround. The case has only come up now. The second one is that Uber has been in the news for all the wrong reasons, where Uber was accessing location even after completing the trip. I don't think it's black and white.

My concern is that when you speak to them, they dismiss it on a technolog-

ical ground, else they say please fight this out in California. These big tech companies shoudl we have a robust enough framework to bring them to court.

Justice Srikrishna: whoever operates in India is subject to Indian law.

NSDL representative: With regards to consent, there should be a lifecycle of the consent, and they ought to take a periodic consent. Many times consent is drafted, the individual is not allowed to say no. For example, if I'm giving KYC data to a bank account, I could be asked to give the data to the credit card. In terms of revocation of content, I shoul dbe allowed to revoke consent. In terms of data collection, does the consent also apply to other information that I have not submitted, which they have to acquire from the third party.

In case someone dies there should be an heir to the data. The heir should have a legal authority to take authority to take action. So many times, the data of the dead can be misused again the living. Protection of the livign because of the data of the dead is also important here.

What happens if I collect data from the Internet, why can't I use the data? how can you say its misuse of data?

Medical data and financial data is contradicting: if I'm in a coma and someone needs my medical records, will my consent be required?

USIBC representative: supports a light touch regulation with freedom of movement of data. It recommends that the govt prepares privacy principles similar to OECD.

Nikhil (that's me): made a point about mass surveillance and why governments need to be governed by this law, and there were judicial oversight mechanisms which were not allowed as amendments to the Aadhaar act; the need for data minimisation, poor implementation of Aadhaar which is putting citizens at mass risk; also the problems with mass customization and predatory behaviour; the need for consent because consent is a switch (countering Malavika Raghavan's previous statement about consent primarily serving the purpose of notice).

Another Speaker: Sector regulators have sometimes been bought in. It would be a problem if we allow sectoral regulators to determine granular parts of the law. We ould end up areas where the same individual and same data is seen under two microscopes. The last point is of due sunset clauses. Will we do it for one year, five years. Having such a clause would help such a law be futuristic, where we can go back to this law every three years.

Justice Srikrishna: You're talking about a suset clause for the law?

Speaker: There could be clauses that would need to be checked for relevance periodically.

Suchana, Hindustan Unilever: On the point on consent around medical issues, as a corporation we often are at crossroads where we have to decide how much

to share when one of our people needs medical information. Thus, taking informed consent when I am the custodian. The law can provide exceptions for reasonableness considering exigencies, and security measures that I need to take before sharing.

Justice Srikrishna: the whole idea is for everybody to understand what everyone is saying

Malavika Raghavan: I wanted to provide a couple of ways in which we could look at the liability section. There's a section on accountability and enforcement tools. If we look at the objectives to promote the agency of people,

Justice Srikrishna: benefit and empower, give them control and prevent harms

Malavika Raghavan: The formulation that we're thinking through are a list of rights, which will be the fount of the obligations. You must take consent, you must allow access to data, there should be a statutory ... you could allow strict liability standards for specific rights. The good thing about strict liability, if you're thinking about insurance, it always need a strict standard. For the ex ante measures, you should have strict liability. The second level is this idea of harms, and there are regulators who have started defining harms: They've worded it widely in terms of actual injury or loss. You can have a reasonable efforts standard for this. We should have a reasonable clear standard for the right to informational privacy. The interesting thing is that we are not actively misusing data. The IT Act does so. None of this is that we are new to. In India, nothing will work because we don't have regulatory capacity.

Justice Srikrishna: We are concerned with normative standards.

Malavika Raghavan: Firstly when we think about the powers of the regulators, we want to make the case for ex ante supervision before the breach. Every time we've had intersectoral coordination in case of ULIP. The FLRC recommendations did look at private and public warnings. You could have a range of investigative powers. It is useful for the regulators to escalate some of these things. IF you have a regulator that speaks softly but carries a big stick is in the interest of the ecosystem. Two other things: a complaints database. The consumer regulators in the US. Aadhaar already has a complaints database. You could look technology to mine this data and have a heatmap for which types of agencies. The other is the notion of reg-tech.

Justice Srikrishna: There could also be a complaint about the privacy of the organisation where it could be used to victimise.

Malavika Raghavan: It could use differential privacy and a frequency graph. The other issue is the accountability of the regulator. It could be the enforcement directorate. That transparency is important to signal the market. Ex Ante these things need to be looked at.

All types of national identifiers, there need to be some restrictions around their disclosure and use. These should be used limited. There was a final point around

data controllers. Because we talked about entities interacting with consumers who are not the controller. Any entity interacting with the consumer collecting the data. The reason why this is important: they only perform an aggregation.

Justice Srikrishna: There is one entity which collects data, does not process, hands it to A, B, C, and if there's a breach at the end point who should be held liable?

Malavika Raghavan: Data controller is the person who is collecting data from the user. And the person for whom the data is collected. Everyone is a processor or a controller, and there should be joint liability.

Rajat Moonra: In IPC the notion of accomplices is already there.

Vickram Krishna: We've seen in India, that the amount of concentration of corporate power is following the same pattern as conglomeration in Europe. The second is that we all take it for granted that Antarctica is melting. We have arguments about why it is melting. But people are convinced that it is because of human action. So we don't take it for granted. What I found missing in the white paper is the possibility that we have some other way of managing our production, our productivity. We don't think of civil society as being productive. That's not the way it used to be. There's no recognition of it in the white paper.

This is the new production.

Speaker: There is one way in which it leads to data protection. Any centralisation leads to data vulnerability. What are the ways in which citizens can be empowered is a distributed model. Empowerment of citizens. What is the time when data protection would enhance.

Justice Srikrishna: Let's forget the law totally. Today someone will ask you your name etc etc. Person might do it because they want to give you better service.

Speaker: Instead of a single large silo.

Srikrishna: Data collection is a fact of life. There should be a right for people to say don't do it, don't do it for this purpose, use it for this purpose.

Speaker: We can set the direction in which it is moving. I want to keep my wallet in my hand.

Other speaker: About the exemptions proposed in the white paper. There should be certain minimum obligations. For example if you have for personal use in household purposes, for example matrimonial lists which can be published online. You could have an app like truecaller. Soe obligations nad restrictions need to be kept.

On national security, you have the DNA data bank, for investigative purposes, but it has huge potential for violation of privacy.

Srikrishna: It's to do this more scientifically. The DNA data bank. It should be done or not be done?

Speaker: The first draft suggested collected the data of everyone.

Srikrishna: The criminals are limited scenes of crimes, for the purpose of modus operandi.

Speaker: The second draft removed that and restricted it to criminals. The data protection authority should have the power to prevent it. Then there are searches of devices at the borders.

Update: Asheeta Regidi, a technology policy lawyer says that these were her points, and clarifies further:

"My point was on the exemptions- that they shouldn't be drafted too broadly, and minimum obligations and restrictions must be in place. One example is the exemption of personal use/ household purposes- where you can have a matrimonial list created for circulation among private members of a society (a personal use), and is then published online via a blogpost (a privacy violation). Similarly, address books could be exempted as a personal use, but you have an app like Truecaller which collects it into a publicly accessible database.

A second exemption is that of investigative purposes/ national security. These should not be drafted in a way that prevents the Data Protection Authority from acting against a state violation of privacy. An example is that of the proposed DNA databank that is to be created for investigative purposes, but has huge potential for privacy violations (looking at the first version of the draft bill).

Another example is the border searches of devices as seen in the US, which could be exempted in the name of national security. It is important that privacy obligations such as collection limitation, storage limitation, data erasure, etc. (and not just purpose limitation, as specified by Justice Sri Krishna) apply to the data collected at such points. The DPA must retain the authority to act against such violations."

Another speaker: DNA and fingerprints are collected by police authorities. At times govt has an exemption. But the liability for them is much lesser than for the normal people at large. The standard of liability should be the same.

Manoj: Like investor protection fund, we can have a consent protection fund. It will reimburse users in case of breaches as a compensatory measure. So that unnecessary prohibition of data. Secondly, self regulation.

Rahul Sharma: On the aspect of building in privacy by design. Singapore has it in its national cyber security strategy. Should it be law or a part of standards. There are roles for sectoral regulation, etc etc, and then try and figure out what everyone will do. Usually laws do not have a sunshine period. We should have this.

GDPR is increasing the cost of compliance, without enhancing security and privacy. There has to be a proportionate increase of security. The cost gets transferred to users. Data localisation was a protectionist strategy. We have an

opportunity to counter this. The government can ensure it for its data, but not for the private sector.

Nikhil from UTV: While we support notice and consent, the restriction that consumer facing industries that are not able to take consent, but consumers are willing to get it. Two year timeline for implementation of the law. It'll take

Suresh Menon: At Maharashtra government, we're setting up blockchain. Currently I can only way I can improve it improve my SLAs. We should come out with guidelines of distributed computing, for deleting.

Anupam Saraph: I want to thank you for actually saying that you'll be technology agnostic. I'd like tyou to be agnostic to words that we import fro m technology. One is the idea of ekyc. ekyc and kyc are two different things. ekyc can be used in N number of places, and there is no way this can be prevented. This boils down to import of concept from technolog. The second is the idea of identification. There is no idea of identification in authentication. To use authentication where identification is required. I'm going to stop here because this is important when we are going to talk about data protection pertaining to the digital space. In digital, all of these concepts, you don't think about how you have changed the responsibiltiy of the partners who have been transacting manually, and sometimes you end up throwing out the responsibility from anyone. It's important that we understand the business process. It has nothing to do with technology. By digitalisation they should not be able to throw out responsible parties from the process. Branch manager used to be responsible for opening an account. With Ekyc, no one is responsible.

*

(Note: In case you spoke at this event and you want to share additional points or share corrections, please feel free to mail me at nikhil@medianama.com. We'd be happy to append additional points or clarifications with the original text above. If you took notes and published them somewhere, please share with us, and we'd be happy to link out to them)

Medianama Expert comments

- Abhishek Malhotra and Bagmisikha Puhan
- Divij Joshi
- Jyotsna Jayaram
- Nikhil Pahwa
- Nikhil Sud
- Pallavi Bedi
- Rahul Narayan
- Sajan Poovayya and Priyadarshi Banerjee
- Smitha Krishna Prasad
- Smriti Parsheera
- Trehan
- Vaneesha Jain
- Vrinda Bhandari
- Vrinda Bhandari and Rishab Bailey

Additional Commentary on the Bill

- Dvara Research
- Jochai Ben-Avie and Udbhav Tiwari (on behalf of Mozilla)
- Vrinda Bhandari
- Divij Joshi
- Nikhil Pahwa

Internet Freedom Foundation

This brief has been authored by SaveOurPrivacy volunteers (Maansi Verma, Vrinda Bhandari, Gautam Bhatia, S. Prasanna, Raman Chima, Anushka Jain, Apurva Singh, Shreya Tiwari, Ishika Garg and Apar Gupta,) to assist legislative engagement.

Other research from

- Ikigai law
- Dvara Research
- SFLC
- DSCI
- SaveOurPrivacy.in