Submission to the Joint Parliamentary Committee on the Personal Data Protection Bill (2019)

IT for Change

February 2020

A legal framework on the protection of personal data is imperative for empowerment, progress and innovation in the 21st Century (Report of the Committee of Experts under the Chairmanship of Justice Srikrishna, 2018). In the words of Justice Chandrachud in *Justice K.S. Puttaswamy (Retd.) vs Union of India (2017)*, the "(f)ormulation 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."

We appreciate the expansion of the definition of personal data to include inferred data (Section 3(28)), the introduction of a right to erasure (Section 18), notifying the class of 'significant data fiduciaries' for data protection impact assessment (Section 27), and 'a privacy by design' policy (Section 22) in the 2019 version of the Personal Data Protection Bill. However, we are concerned about the absence of checks and balances in regard to state processing of personal data on grounds other than consent.

We recognise that state access to non-personal data is essential for carrying out governance functions in public interest and the powers bestowed by Section 91(2) on state agencies to demand mandatory sharing of critical non-personal data sets currently locked up by Big Tech. However, we do hope that the imminent report of the Committee of Experts deliberating norms for data governance will pave the way for specific legislation that while enabling the state to issue directions to data fiduciaries/processors to mandatorily share non-personal data sets for legitimate public policy functions, also balances other competing claims in relation to such non-personal datasets.

We also submit that the Bill uphold the independence and autonomy of the Data Protection Authority. We recommend the restoration of the independent Selection Committee for appointing the members of the DPA, as outlined in the Justice Srikrishna Committee Report (2018).

The comments below address IT for Change's concerns and aspirations for the data protection law. Our inputs are guided by the conviction that the fundamental and overarching principles of lawfulness, legitimacy, necessity and proportionality in state processing of citizen data as underlined in *Justice K.S. Puttaswamy (Retd.) vs Union of India (2017)* and the vision of a free and fair digital economy founded on the informational autonomy of citizens constitute the touchstone for every single provision of our personal data protection law. We wish to draw your attention particularly to the comments on the treatment of non-personal data (Sections 91), the inclusion of de-anonymisation as an offence (Section 82), grounds for data processing without consent (Sections 12, 13 and 14), voluntary verification of identity enabled by social media intermediaries (Sections 26 & 28), exemptions to State agencies (Section 35 & 86), and the constitution of the Selection Committee that appoints the members of the Data Protection Authority (Section 42).

Summary of Important Recommendations

Topic	Summary
On the treatment of non-personal data (Section 91)	As per Section 91, the Central Government may direct any data fiduciary or data processor to provide access to non-personal data ("NPD"). In the current context, access to non-personal data may be needed for a range of state functions and not just for "better targeting of services" or "formulation of evidence-based policies". For example, smart traffic management by traffic authorities will benefit immensely from access to non-personal data sets on traffic flows that are currently with private platforms such as Google and Uber. The current wording of 91(2) is too narrow and does not account for such instances, and we recommend that the scope of public interest claims in data be broadened. We do hope that the imminent report of the Committee of Experts deliberating norms for data governance will pave the way for specific legislation that while enabling the state to issue directions to data fiduciaries/processors to mandatorily share non-personal data sets for legitimate public policy functions, also balances other competing claims in relation to such non-personal datasets.
On acknowledging de-anonymisation as an offence of re-identification (Sections 82, 3 and 25)	Section 82 must also acknowledge intentional re-identification through processing of anonymised data as an offence. A definition of "deanonymisation" should be added to Section 3. The obligations for reporting of personal data breaches under Section 25 should also explicitly cover instances of unintentional reidentification or deanonymisation of deidentified/ anonymised data that is in the control of any third party.
On qualified exemptions for research, archiving or statistical purposes (Section 38)	Section 38 permits the Authority to exempt personal data processing for research, archiving or statistical purposes from 'any application of any of the provisions of this Act', subject to regulations. It is suggested that the scope of this exemption be narrowed so that even in the case of personal data processing for research, there are certain foundational sets of rights and obligations of the data principals and data fiduciaries, respectively, that cannot be derogated from.

Consent Managers (Sections 3 and 23)	The relationship between a consent manager and a data principal relies upon the consent manager's acting in the best interests of the data principal. It is therefore important for the broad contours of this relationship to be specified in law, in consonance with the principles laid down in the Srikrishna Committee Report. In this respect, it is necessary to define a consent manager and delineate its scope of work, functions, interface etc. It is suggested that a consent manager be defined in the Bill in the definitional clause or Section 3 and its powers to collect, store and use personal data of data principals be narrowed in Section 23, so that consent managers are permitted to process personal data only for the purpose of discharging their specific function of mediating consent.
Levying fees on processing requests pertaining to data rights (Section 21)	The exercise of data rights should not be curtailed on the grounds of burdensome fees charged by data fiduciaries, except in rare instances for reasons to be given in writing. We recommend that the power of data fiduciaries to levy fees as permitted in Section 21 be limited to instances where the request from a data principal is unreasonably and unduly burdensome for the data fiduciary to comply with.
Exemptions to State agencies (Section 35, 36 and 86).	The deletion of Section 35 is recommended for it would be "open to the authorities to be arbitrary and whimsical"[1] without the application of the Data Protection law on their actions. Section 36 is correspondingly modified to incorporate higher standards for executive exemptions. It is recommended that Section 86 be deleted. Stand-alone, and read in combination with Section 35, the scope of the directions that may be issued under Section 86 suffers from ambiguity due to overbreadth.
Grounds for data processing without consent (Sections 12, 13 and 14)	It is recommended that Section 12 be amended such as to remove non-consensual data collection from the pale of exclusively executive action. Non-consensual Personal data processing by state agencies must be proportionate to a legitimate aim pursued under the law. Employers are not merely data fiduciaries, they have a greater degree of control over their employees than data fiduciaries. It is recommended that Section 13 be changed to include additional safeguards and to balance the rights over personal data owed to an employee vis a vis their employer.

[1]Shreya Singhal v Union of India, W.P. No. 167 of 2012

	Employees are too often subject to monitoring and surveillance at their workplaces. Such practices are inimical to the dignity and humanity of workers. It is thus, recommended, that a provision be added in the Code of Ethics in Section 50 towards this end. Section 14(1) needs to be amended for clarity. Further, the list of reasonable purposes in Section 14(2) should be deleted. It is especially noted that "(g) processing of publicly available personal data" creates ambiguities such as a lack of clarity as to the meaning of "publicly available". Equally, it is noted that the "(f) operation of search engines" brings in ambiguity about what "operation" entails, which may have significant impacts on rights of data principals. These two categories have been included without any reasoning or rational nexus being provided for such inclusion. Given that this provision provides a *carte blanche* for processing of personal data without consent, these purposes cannot be included in such a provision.
Selection Committee for the Data Protection Authority (Section 42)	We recommend that Section 42 be modified in order to reinstate the selection committee as envisaged under the Justice Srikrishna Committee Report (2018),[2] and subsequently provided for in the 2018 PDP Bill. The inclusion of a member of the judiciary ensures the independence of the selection committee, and this is bolstered by the inclusion of an expert of repute. The inclusion of an expert of repute also ensures that the selection committee is well-equipped to take into account technical considerations while appointing members of the Authority.
On transparent functioning of the Data Protection Authority (Section 49)	The Authority is a body tasked with the extremely important function of creating and ensuring an ecosystem of responsible data handling. Therefore, we suggest modifying Section 49 in order to impose a transparency obligation on the Authority, modelled around the transparency provisions in the establishing legislation of two other sectoral regulators, namely, the Telecom Regulatory Authority of India and the Airports Economic Regulatory Authority of India.

[2]Page 153 of the Srikrishna Committee Report

Voluntary verification of identity enabled by social media intermediaries (Sections 26 and 28)	It is recommended that defining social media intermediaries on the basis of terms such as "users" and "online interaction" should be avoided under this statute. Not only are the terms difficult to define, qualifying social media intermediaries by a threshold of minimum users emerges from an impartial understanding of the origins of disinformation. Therefore, we recommend the deletion of 26(4) and its explanation defining social media intermediaries. The Bill treats this category of social media intermediaries exactly like significant data fiduciaries, except for the additional requirement to enable voluntary verification of notified social media intermediaries or class of social media intermediaries. Such a verification provision does not materially affect personal data protection rights, and should therefore be avoided in this Bill. A requirement for data fiduciaries to enable voluntary verification of identity is better placed in a content regulation law, and not a personal data protection law. Therefore, Section 28 (3) and (4) are deleted.
Bar on processing certain forms of biometric data (Section 92)	This provision has been rephrased for greater clarity. We recommend that the provision read: "No data fiduciary shall process biometric data unless such biometric data has been notified by the Central Government, and is processed in accordance with the law."

INDEX

Table of Contents

Legend:

Recommended deletions are denoted through ~~Strikethrough~~.

Recommended additions are denoted through **Bold**.

Capitalised terms used have the same meaning as assigned to them in the Bill, unless specifically defined herein.

1. On the treatment of non-personal data

1a. Comments on Section 91

Comments on Section 91

As per Section 91, the Central Government may direct any data fiduciary or data processor to provide access to non-personal data ("NPD"). In the current context, access to non-personal data may be needed for a range of state functions and not just for "better targeting of services" or "formulation of evidence-based policies". For example, smart traffic management by traffic authorities will benefit immensely from access to non-personal data sets on traffic flows that are currently with private platforms such as Google and Uber. The current wording of 91(2) is too narrow and does not account for such instances, and we recommend that the scope of public interest claims in data be broadened.

Proposed Text in Bill	**Recommended Text**
Section 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. (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. (3) The Central Government shall disclose annually the directions, made by it under sub-section (2), in such form as may be prescribed.	Section 91 **(1) Nothing in this Act shall prevent the Central Government from framing any policies for a free, fair and equitable digital economy, insofar as they do not govern personal data.** **(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 that is required in public interest to carry out any authorised function of the state, including policy development, in such manner as may be prescribed by the Authority.**

Rationale for the Recommendation

Policy measures that leverage NPD for the growth, security and integrity of the digital economy may be agnostic to economic and social inequality

and economic unfreedoms. We seek policies through which the government can use NPD for promoting individual and collective economic wellbeing. We have modified 91(1) accordingly.

Going forward, such policies must be backed by a robust legal framework for the governance of non-personal data that balances multiple and competing claims of data sources and data collectors towards the larger public interest. We hope that the imminent report of the Committee of Experts deliberating norms for data governance will pave the way for specific legislation that while enabling the state to issue directions to data fiduciaries/processors to mandatorily share non-personal data sets for legitimate public policy functions, also balances other competing claims in relation to such non-personal datasets.

Section 91(2) has been amended to broaden the scope of public interest claims in non-personal data.

2. On Penalties for breach of anonymisation

2a. Comments on Section 82

Comments on Section 82	
Section 82 penalises intentional re-identification and processing of de-identified personal data. Research has shown that anonymisation is not a foolproof safeguard against reidentification,[3] We propose, therefore, that Section 82 must also consider intentional reidentification through de-anonymisation as an offence. Importantly, while re-identification in the case of de-identified data may not be an offence if undertaken by (i) the data fiduciary or data processor concerned, or (ii) if done with the consent of the concerned data fiduciary or data processor, this does not apply to re-identification of anonymised data or de-anonymisation.	
Proposed Text in Bill	**Recommended Text**
Section 82	Section 82
(1) Any person who, knowingly or intentionally—	(1) Any person who, knowingly or intentionally—
(a) re-identifies personal data which has been de-identified by a data fiduciary or a data processor, as the case may be; or	(a) re-identifies**, or processes after re-identification**, personal data which has been de-identified by a data fiduciary or a data processor **not being such data fiduciary or data processor, without the consent of such data fiduciary or data processor,** as the case may be; or
(b) re-identifies and processes such personal data as mentioned in clause (a), without the consent of such data fiduciary or data processor, then, such person shall be punishable with imprisonment for a term not exceeding three years or with a fine which may extend to two lakh rupees or both.	**(b) de-anonymises, or processes after de-anonymisation, personal data which has been anonymised by a data fiduciary or a data processor, as the case may be;** 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—	(2) Nothing contained in sub-section (1) shall render any such person liable to any punishment under this section, if he proves that—
(a) the personal data belongs to the person charged with the offence under sub-section (1); or	**(a) he is the data principal whose personal data is in question; 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.

[3]Why 'Anonymous' Data Sometimes Isn't, available at https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/

(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.	

Rationale for the Recommendation

Since anonymised data has been in use by private parties, without any protections or safeguards, and is increasingly sought to be used by the state for public functions under the PDP Bill, it has to be adequately protected and data fiduciaries need to be disincentivised from misusing it or handling it negligently. Thus, the offence of re-identification is sought to be modified such that the offence of de-anonymisation is added.

In the phrase 'personal data belongs to the person charged with the offence' from the proposed Section 82(2)(a), it is unclear to whom the personal data 'belongs'. This generates questions of ownership and property rights in data, which are still in flux. Thus, in accordance with the data protection framework, the primary rights and control is sought to be granted to the data principals to consent for re-identification of de-identified data.

It may be added that many jurisdictions provide a framework to deal with anonymised data[4] and some jurisdictions are mulling over laws to provide a framework to deal with anonymised data.[5]

[4]Japanese Act on Protection of Personal Information, Sections 36-42, https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf; Section 171 (2), UK DPA, http://www.legislation.gov.uk/ukpga/2018/12/section/171/enacted

[5]Canadian privacy law *Personal Information Protection and Electronic Documents Act*, https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-ai/pos_ai_202001/#fn39-rf; Australian privacy law, Privacy Act 1988, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1047, though the Bill has lapsed due to the end of the session.

2b. Comments on Section 3 in view of Section 82

<table>
<tr><td colspan="2">Comments on Section 3 in view of Section 82
There is ample recognition of the potential reversibility of data anonymisation even amongst law making bodies.[6]
Keeping in mind the possibility of reversal of anonymisation, a new definition of ‘de-anonymisation’ is proposed.</td></tr>
<tr><td>Proposed Text in Bill
Does not exist.</td><td>Recommended Text
To be added in Section 3
“de-anonymisation” means the process by which a data fiduciary or data processor, or any other person, may reverse, undo or change the effect of a process of anonymisation to render such data as personal data;</td></tr>
<tr><td colspan="2">Rationale for the Recommendation
The addition of the definition of de-anonymisation is the first step towards incorporation of an entire framework dealing with anonymised data. Re-identification is penalised in Section 82 of the Bill and it should also include de-anonymisation. Thus, to that extent, the provision is sought to be modified.</td></tr>
</table>

[6]Opinion 05/2014 on Anonymisation Techniques, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf, Justice Sri Krishna Committee Report, pg. 34

2c. Comments on Section 25 in view of Section 82

<table>
<tr><td colspan="2">Comments on Section 25 in view of Section 82

The obligations for reporting of personal data breaches under Section 25 should also explicitly cover instances of unintentional reidentification or deanonymisation of deidentified/anonymised data that is in the control of any third party. To incorporate this understanding, Section 25 is sought to be modified and new provisions are added.</td></tr>
<tr><td>Proposed Text in Bill</td><td>Recommended Text

Section 25

(8) In the event that a personal data breach occurs due to processing of anonymised data or de-identified data, the person processing such data shall be subject to the obligations of the data fiduciary in this section.

(9) For all personal data breach arising in sub-section (8), the Authority may take additional action, as provided under Section 82, without prejudice to its powers under this section.</td></tr>
<tr><td colspan="2">Rationale for the Recommendation

Since the obligations under Section 25 are fulfilled by a data fiduciary, it is important to lay down a framework such that the person whose actions lead to data breaches through unintentional re-identification/deanonymisation is also held responsible as a data fiduciary. To that extent, the Section has been modified.

The Authority is in a position to decide the most suitable action to be taken regarding any case of deidentification/ de-anonymisation, its consequences and the harm caused by it. Thus, the steps taken under Section 25 are without prejudice to its powers under Section 82, as suggested.

Since changes have been suggested to the entire framework of the processing of anonymised data, suitable changes are required to Section 2(B) for consistency, to add reference to anonymised data as mentioned in Sections 25 and 82.</td></tr>
</table>

3. Qualified exemptions for research, archiving or statistical purposes

3a. Comments on Section 38

Comments on Section 38	
The importance of an exemption for processing of personal data to be used for research purposes has been outlined in the Justice Srikrishna Committee Report (2018)[7] and *Justice K.S. Puttaswamy (Retd.) vs Union of India (2017),*[8] Section 38 exemptions should only be for such research activities that promote the public good, devoid of mercenary motives. The Srikrishna Committee Report has understood 'research' to include scientific, academic and historical research.[9] The Bill should also include literary and artistic works. Section 38 permits the Authority to exempt personal data processing for research, archiving or statistical purposes from 'any application of any of the provisions of this Act', subject to regulations. It is suggested that the scope of this exemption be narrowed so that even in the case of personal data processing for research, certain foundational sets of rights and obligations of data principals and data fiduciaries continue to hold. This position is also supported by the GDPR.[10]	
Proposed Text in the Bill	**Recommended Text**
Section 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; (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	Section 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; (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

[7]pg 121, the Srikrishna Committee Report

[8]para 69-73, Justice K.S. Puttaswamy (Retd.) vs Union of India (2017)

[9]pg 137, the Srikrishna Committee Report

[10]Article 14, 5, 89

of processing can be achieved if the personal data is in de-identified form; (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.	can be achieved if the personal data is in de-identified form; (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, **(f) the research, archiving, or statistical purposes are bonafide and non-commercial** 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. **Further, the Authority shall not exempt such notified class of research, archiving, or statistical purposes from Sections 4, 6, 8, 16, 17, 22 and 24.**
Rationale for the Recommendation The Justice Srikrishna Committee Report (2018) balanced exemption for research and the right to privacy by placing research in the context of its societal and commercial purpose.[11] Large technology companies have dedicated research arms.[12] It is important that research carried out by "Big Tech" be scrutinised at a higher standard as compared to an academic endeavour or research. Such commercial research is usually opaque, and can have far reaching consequences such as was evident in the Cambridge Analytica scandal and also lead to biased outcomes for public policymaking.[13] Thus, the Authority must exercise reasonable discretion and not exempt commercial research from any provisions of the law. The scope of exemptions of personal data processing for research, archiving or statistical purposes has been narrowed. Certain privacy principles as well as obligations of the data fiduciaries have been added to safeguard key rights and ensure that such provisions will also instruct the decision of the Authority to exempt certain provisions.	

[11]121, the Srikrishna Committee Report

[12]A Preliminary Opinion on data protection and scientific research, available at https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf

[13]https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf, for example, EU's 2019 Copyright Directive(Directive (EU) 2019/790) excludes commercial research from the purview of copyright exemption.

4. On the definition and powers of consent managers

4a. Comments on Section 3 and 23

Comments on Section 3 and 23 The relationship between a consent manager and data principal relies upon the consent manager's acting in the best interests of the data principal. It is therefore important for the broad contours of this relationship to be specified in law, in consonance with the principles laid down in the Srikrishna Committee Report. In this respect, it is necessary to define a consent manager and delineate its scope of work, functions, interface etc. It is suggested that a consent manager be defined in the Bill in the definitional clause or Section 3 and its powers to collect, store and use personal data of data principals be narrowed in Section 23, so that consent managers are permitted to process personal data only for the purpose of discharging their specific function of mediating consent.	
Proposed Text in Bill Section 23 (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. 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	**Recommended Text** Add in the definition clause, Section 3 **"Consent Manager" means a data fiduciary that enables a data principal to gain, give, withdraw, review and manage his consent through an accessible, transparent and interoperable platform and is further governed as provided in Section 23.** Section 23 **(4) The consent manager shall not collect, store or use any personal data of the data principal, other than the personal data required by it to carry out its function.**[14] (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. ~~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.~~

[14]Report, pg 39, Section 3 (iv), Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016, https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598

accessible, transparent and interoperable platform.	

Rationale for the Recommendation

Currently, the definition, duties and rights of a consent manager are spread across the Bill with inconsistency in explanation. For example, the definition of a consent manager provided as an Explanation to Section 23(5) of the Bill applies the definition **only to that provision**. To that extent, a consent manager is undefined for the rest of the provisions using the concept of this entity in Section 21 or Chapter V which introduces the concept. This creates ambiguity and is sought to be changed.

While the consent manager's function under the Explanation is restricted to dealing with consent, the functions envisaged under Chapter V are wider and import a role of the consent manager as an agent of the principal, to the extent of exercising certain rights under Chapter V. Thus, the scope of the functions to be carried out by the consent manager have to be clarified and restricted to managing consent only.

5. On fees that can be levied by data fiduciaries for requests from data principals

5a. Comments on Section 21

Comments on Section 21	
Chapter V lays down certain rights exclusive to the data principals such as the right to be forgotten, right to correction, etc. The conditions and modalities to operationalise these rights are delineated in Section 21. Section 21(2) provides that the data fiduciary may charge such fees as may be specified by regulations. Additionally, it also flags that no fee may be charged in respect of rights referred to in clause (a) or (b) of sub-section (1) of section 17 or section 18. The said method of operationalisation makes the exercise of rights contingent upon payment of fee and redefines the right as a service[15]. Although there is an existing precedence for the payment of fee in lieu of exercising these rights, as it was mentioned in the Justice Srikrishna Committee Report (2018)[16], the GDPR[17], UK Data Protection Act, 2018[18] ("UK DPA") and the Japanese Act on Protection of Personal Information[19]. However, the requirement of fee is subject to justifications such as unreasonable burden, difficulty imposed on the data fiduciary, or on the actual expenses undertaken by the data fiduciary. Such safeguards are required in the present law to ensure that digital rights increasingly become a reality for people.	
Proposed Text in Bill	**Recommended Text**
Section 21(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.	Section 21(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. **Provided further that such fee may be charged only if the request is unreasonably and unduly burdensome for the data fiduciary to comply with. In such a case, the data fiduciary shall provide the reasons to charge a fee at the time of responding to the data principal.**

[15]GDPR- No More Data Subject Access Request Fees, available at https://www.skillcast.com/blog/gdpr-no-more-data-subject-access-request-fees
[16]Report, pg 70
[17]Article 12 (5), GDPR
[18]Section 12, UK Data Protection Act, 2018 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/

Rationale for the Recommendation

It may make it difficult for certain data principals to seek execution of such rights and may be perceived as unfair, especially when the exercise of rights is not unreasonably burdensome for the data processors or data fiduciaries to comply with. The exercise of data rights should not be curtailed on the grounds of burdensome fees charged by data fiduciaries, except in rare instances for reasons to be given in writing. Thus, certain governing principles and conditions are added to provide the instances of where a fee may be charged. This may inform the task of the Authority in determining reasonableness.

[19]Article 33, Japanese Act on Protection of Personal Information, https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf

6. On exemptions for state agencies

6a. Comments on Section 35 and 36

Comments on Sections 35 and 36

Sections 35 of the Bill confer the Central Government with the power to exempt any agency of the Government from application of any or certain provisions of the Bill, the legitimate requirement sought under this Section should be fulfilled through a separate law as envisioned through the Srikrishna Committee Report.[20]

(I) Requirement of legality, necessity and proportionality

The Bill departs from the comparable provisions in the Personal Data Protection Bill, 2018 ("2018 Bill") by omitting the requirements of necessity and proportionality as stated by the Supreme Court in *Justice K.S. Puttaswamy (Retd.) vs Union of India (2017)*. These interests of necessity and proportionality were also noted in the Srikrishna Committee Report.[21] The removal of these requirements is unjustified and unwarranted.

(II) Establishment of adequate oversight mechanism

Section 35 states that the procedure, safeguards and oversight mechanism will be "as prescribed". This is a serious concern of excessive delegation as the framing of the oversight mechanisms has been left to the Executive, thereby bypassing any Parliamentary or Judicial oversight regarding this matter. The concern and requirement for judicial and parliamentary oversight have been explicitly noted in the Srikrishna Committee Report.[22]

(III) Extensive scope of exemption under Section 35

The scope of the exemption under Section 35 is inordinate as it enables the Central Government to exempt the application of the entire Bill on such agencies as the Central Government may choose. Even Section 42 of the 2018 Bill, while exempting the application of the 2018 Bill, provided that Section 4 (on fair and reasonable processing), Section 31 (security safeguards), and Chapters IX (Exemption), X (Data Protection Authority), XI (Penalties and Remedies), XII (Appellate Tribunal), XIII (Offences), XV (Miscellaneous) would apply. This is similar to Section 36 of the current Bill and there is no analogous provision in the 2018 Bill to Section 35 of the current Bill.

Section 26 of the UK DPA[23] which incorporates the "national security" and "defence" exemption (there is no public order, sovereignty, friendly relations exemption), exempts portions of the GDPR except for (i) Article 5(1)(a) (lawful, fair and transparent processing), so far as it requires processing of personal data to be lawful; (ii) Article 6 (lawfulness of processing); and (iii) Article 9 (processing of special categories of personal

[20]Page 128 of the Srikrishna Committee Report
[21]Page 121, 127, 128 of the Srikrishna Committee Report
[22]Page 128 of the Srikrishna Committee Report
[23]Section 26, UK Data Protection Act, 2018, http://www.legislation.gov.uk/ukpga/2018/12/section/26/enacted

data).

The GDPR itself does not contain any provision which provides an exemption from application of the entire Regulation.

(IV) Requirement for detailed regulations to ensure safeguarding of individual rights

While we acknowledge the necessity for an exemption from certain provisions of the Bill for the purposes stated in Section 36 (a), the exemption must be provided with safeguards to ensure that the exemption is used only for legitimate and well-defined purposes and for limited periods of time.[24] Furthermore, as noted by the Srikrishna Committee Report, cases involving the processing of sensitive personal data should be subject to a greater degree of oversight.[25] In fact, the GDPR does not apply to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.[26] The processing of personal data for such purposes is separately governed by Directive (EU) 2016/680 which contains extensive provisions to ensure safeguards for the rights of the data principal.

Proposed Text in Bill	**Recommended Text**
Section 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.	**Delete Section 35** Section 36 The provisions of Chapter II except section 4, **section 5**, **and section 6,** 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 **integrity and sovereignty of India** or prevention, detection, investigation and prosecution of any offence, or any other contravention of any law for the time being in force; **Provided that the exemption granted in this subsection shall apply only to the Central Government or a State Government or any officer specially authorised by the Central Government**

[24]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>
[25]Page 133 of the Srikrishna Committee Report
[26]Recital 19, GDPR.

Section 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.	**or the State Government, as the case may be.** **Provided further that the exemption granted in this subsection shall not apply unless the processing of personal data is necessary for a legitimate and well-defined purpose, and is proportionate to the interests sought to be achieved.** **Provided further that personal data processed for purposes listed in subsection 36 (a) 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 the future.** 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.

Rationale for the Recommendation

Given the excessive and inordinate scope of powers provided to the Central Government in Section 35 we recommend that Section 35 be removed from the Bill. However, the requirement for exemption of application of certain provisions of the Bill in the interest of the integrity and sovereignty of the State is acknowledged, and we have accordingly amended Section 36(a) of the Bill.

We have also inserted a number of provisos to the application of Section 36(a) of Bill to ensure that:

(a) the exemption is utilised only by law enforcement agencies or agencies of the government;

(b) the exemption is exercised in accordance with the limits set by the Supreme Court in *Justice K.S. Puttaswamy (Retd.) vs Union of India (2017)*, and

(c) the data collected by authorities is only stored for a reasonable period of time in light of the purpose the data is collected for.

Furthermore, we have also removed Sections 5 (limitations on purpose of processing of personal data) and Section 6 (limitation on collection of personal data) of the Bill from the ambit of the exemptions in Section 36.

6b. Comments on Section 86

Comments on Section 86
The Central Government has been granted the power to issue directions and frame policies in Section 86. A direction is a particular kind of delegated legislation by the executive with legally binding effect.[27] It is suggested that Section 86 be removed in its entirety.[28] When read in combination with Section 35 the scope of the directions to be issued under Section 86 suffers from ambiguity due to overbreadth. It is necessary to ensure the independence of the Authority, as it also exercises regulatory powers over government agencies. The clause, as it currently stands, provides the Central Government the power to override the discretion and expertise of the Authority. This harms the functional independence of the Authority.[29] Thus, it is recommended that the provision be deleted.

[27]P.B. Mukherjee, "Delegated Legislation." *Journal of the Indian Law Institute*, www.jstor.org/stable/43949623.

[28]Justice Srikrishna Committee Report, pg 156.

[29]Regulatory Management and Reform in India, Background Paper for OECD, available at https://www.oecd.org/gov/regulatory-policy/44925979.pdf, pg 19.

7. On grounds for processing of personal data without consent

7a. Comments on Section 12

Comments on Section 12 Section 12 (a) and (b) provide for exemptions from the requirement of consent in certain cases. However, it is unclear why certain State functions are given special treatment under Section 12 (a) when the State may legitimately need to collect data for its many other functions as well. Moreover, as laid down by the Supreme Court in *Justice K.S. Puttaswamy (Retd.) vs Union of India (2017)*, all data collection by the State should be pursuant to aims and objectives under a specific law and must be necessary for, and proportionate to, the objects sought to be achieved by that law. An enabling law should also provide as much clarity about data collection needs, purposes and means as is possible.	
Proposed Text in Bill Section 12 Notwithstanding anything contained in section 11, the personal data may be processed if such processing is necessary,— (a) for the performance of any function of the State authorised by law for— (i) the provision of any service or benefit to the data principal from the State; or (ii) the issuance of any certification, licence or permit for any action or activity of the data principal by the State; (b) under any law for the time being in force made by the Parliament or any State Legislature;	**Recommended Text** Section 12 Notwithstanding anything contained in section 11, the personal data may be processed if such processing is necessary,— ~~(a) for the performance of any function of the State authorised by law for—~~ ~~(i) the provision of any service or benefit to the data principal from the State; or~~ ~~(ii) the issuance of any certification, licence or permit for any action or activity of the data principal by the State;~~ ~~(b) under any law for the time being in force made by the Parliament or any State Legislature;~~ **(a) for the performance of any function of the State under any law for the time being in force made by the Parliament or any State Legislature;** **Provided that such processing is proportionate to a legitimate aim pursued under the law;** **Provided further that the law may contain specific provisions to be followed for such processing of personal data;**

Rationale for the Recommendation

The recommended text in Section 12(a) combines the current text of Sections 12 (a) and (b) of the Bill, and provides for the exemption from the consent requirement of Section 11 in all instances of a State function under any law in force, while ensuring that the exemption is subject to the much higher standard of legislative enactment. This is recommended to remove non-consensual data collection from the pale of exclusively executive action without legal protections. Such a re-framing would enable Section 12 to meet the necessity, proportionality, legality standards for data processing laid down by *Justice K.S. Puttaswamy (Retd.) vs Union of India (2017).*

7b. Comments on Section 13

Comments on Section 13 The Bill presumes that the relationship between an employee and employer is equivalent to that between a data principal and data fiduciary. This assumption needs careful re-examination, due to the added imbalance in power between parties in an employment relationship. The Justice Srikrishna Committee Report (2018) rightly observes 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." This understanding seems to have not been captured in the impugned provision. Employers are not merely data fiduciaries, they have a greater degree of control over their employees than data fiduciaries do over data principals. Hence, additional safeguards are required.	
Proposed Text in Bill Section 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— (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	**Recommended Text** Section 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 **a legitimate and well-defined purpose, and is proportionate to the interests sought to be achieved 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) 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

of the performance of the data principal who is an employee of the data fiduciary. (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.	effort on the part of the data fiduciary due to the nature of the processing under ~~the said~~ sub-section **(1)**. **(3) The Central Government shall make rules or by collective agreements, provide more specific rules to ensure the protection of the rights and freedoms in respect of the processing of personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship,** **(4) Rules or collective agreements made in Sub-section (3) shall have particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the workplace.**
Rationale for the Recommendation The employer is a special kind of data fiduciary with greater responsibilities *vis-à-vis* a special class of data principal, the employee. The addition of 13(3) is derived from Article 88(1)[30] of the GDPR on Processing in the Context of Employment. These areas for regulation of data in the employment context are supplemented by the condition, under Article 88(2), that they will "include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place."	

[30]Art 18, GDPR, https://gdpr-info.eu/art-88-gdpr/

7c. Comments on Section 50

<table>
<tr><td colspan="2">Comments on Section 50 in view of Section 13

ICT mediated workplace surveillance will have a disproportionate impact on the most vulnerable classes of workers[31] to organize for the protection of their collective interests. The right of collective bargaining[32] is an important facet of ensuring humane and dignified working conditions. In the absence of such safeguards, there is a risk to the human rights of workers. Hence, it is important that there should be a code of practice corresponding to Section 13, and among other things, it must incorporate prohibitions on monitoring workers for unionisation.</td></tr>
<tr><td>Proposed Text in Bill</td><td>Recommended Text

To be added to Section 50(6)

processing of personal data under section 13, including prohibitions on monitoring of unionisation and related activity</td></tr>
<tr><td colspan="2">Rationale for the Recommendation

There needs to be incorporated a code of practice dealing with data processing obligations in an employment context. This code of practice should account for prohibitions on the use of data processed in the context of an employment relationship, especially on monitoring of workers' unionisation.</td></tr>
</table>

[31]Gendering Surveillance, available at https://www.genderit.org/resources/gendering-surveillance
[32]Business and Collective Barganing, available at https://www.ilo.org/empent/areas/business-helpdesk/WCMS_DOC_ENT_HLP_CB_EN/lang--en/index.htm

7d. Comments on Section 14

<table>
<tr><td colspan="2">Comments on Section 14

Section 14(1) allows the Authority to specify, through regulations, certain ‘reasonable purposes’ for which personal data may be processed without obtaining consent as specified under Section 11. Sub-Sections (a) to (e) of Section 14(1) mention certain considerations which must be kept in mind by the Authority while framing the regulations. However, from the text of the Section, it is unclear whether the considerations mentioned in sub-Sections (a) to (e) are to be taken into account by the Authority while making the regulations, or by each data fiduciary when such data fiduciary processes the personal data without obtaining consent under Section 11.

Section 14(2) provides an indicative list of what constitutes a ‘reasonable purpose’ for the purpose of Section 14(1). However, there is no reasoning provided for the list of ‘reasonable purposes’ stated in Section 14(2). As the Justice Srikrishna Committee Report (2018) notes,[33] it is for the Authority to provide a whitelist of exempted activities having taken into account the considerations mentioned in Section 14(1).</td></tr>
<tr><td>Proposed Text in Bill

Section 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;

(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.</td><td>Recommended Text

Section 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 <s>as may be specified by regulations, after taking</s> as the Authority may, by regulations specify, having taken 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</td></tr>
</table>

[33] Report, Page 118

14. (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; (c) mergers and acquisitions; (d) network and information security; (e) credit scoring; (f) recovery of debt; (g) processing of publicly available personal data; and (h) the operation of search engines.	context of the processing. **Delete Section 14(2)**

Rationale for the Recommendation

The provision is sought to be modified to ensure there is no ambiguity on whether the duty to keep in mind the considerations specified lies on the Authority or on each data fiduciary.

The Authority is to provide a whitelist of exempted purposes having taken into account the considerations mentioned in Section 14(1). The purposes listed in Section 14(2) have been stated without providing any reasons and objectives, and it is therefore recommended that the indicative list of ‘reasonable purposes’ be deleted.

It is especially noted that “(g) processing of publicly available personal data” creates ambiguities such as a lack of clarity as to the meaning of "publicly available". Equally, it is noted that the "(f) operation of search engines" brings in ambiguity about what "operation" entails, which may have significant impacts on rights of data principals. These two categories have been included without any reasoning or rational nexus being provided for such inclusion. Given that this provision provides a *carte blanche* for processing of personal data without consent, these purposes cannot be included in such a provision.

8. On the selection of the Data Protection Authority

8a. Comments on Section 42

Comments on Section 42 Section 42(2) mentions the composition of the selection committee that will appoint the Chairperson and Members of the Authority. In contrast to the provisions of the 2018 Bill, the committee under this Bill is composed entirely of members from the Executive Branch. The independence of the Authority from the executive should be demonstrated in the composition of the selection committee for the Authority, as the Authority must act as a check on decisions taken by the Government. The independence of the members of Authority shall have as much impact on our ability to be functional democracy as the independence of Election Commissioners or Public Information Officers have. Therefore, the nature and function of the Authority demands that transparency and judicial oversight must inform the selection criteria. Additionally, it is necessary that the selection committee be equipped with adequate knowledge of technological and digital issues to make informed decisions while selecting members of the Authority. Towards this end, the selection committee for the Authority should consist not only of State representatives, representatives of the of members of the judiciary, as well as an expert of repute. This concern is also noted in the Srikrishna Committee Report.[34]	
Proposed Text in Bill	**Recommended Text**
Section 42 (2) The Chairperson and the Members of the Authority shall be appointed by the Central Government on the recommendation made by a selection committee consisting of— (a) the Cabinet Secretary, who shall be Chairperson of the selection committee; (b) the Secretary to the Government of India in the Ministry or Department dealing with the Legal Affairs; and	Section 42 (2) The Chairperson and the Members of the Authority shall be appointed by the Central Government on the recommendation made by a selection committee consisting of— ~~(a) the Cabinet Secretary, who shall be Chairperson of the selection committee;~~ ~~(b) the Secretary to the Government of India in the Ministry or Department dealing with the Legal Affairs; and~~ ~~(c) the Secretary to the Government of India in the Ministry or Department dealing with the Electronics and Information Technology.~~ **(a) the Chief Justice of India or a judge of the Supreme Court of India nominated by the**

[34]Page 153 of the Srikrishna Committee Report

(c) the Secretary to the Government of India in the Ministry or Department dealing with the Electronics and Information Technology.	**Chief Justice of India, who shall be the chairperson of the selection committee;** **(b) the Cabinet Secretary; and** **(c) one expert of repute who has specialised knowledge of, and professional experience, in the fields of *inter alia* data protection, information technology, data management, data science, cyber and internet laws, or data ethics, 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.**
Rationale for the Recommendation We recommend that the selection committee as envisaged under the Justice Srikrishna Committee Report (2018),[35] and subsequently provided for in the 2018 Bill, be reinstated. The inclusion of a member of the judiciary ensures the independence of the selection committee, and this is bolstered by the inclusion of an expert of repute. The inclusion of an expert of repute also ensures that the selection committee is well equipped to take into account technical considerations while appointing members of the Authority.	

[35]Page 153 of the Srikrishna Committee Report

9. On transparency in the functioning of the Data Protection Authority

9a. Comments on Section 49

Comments on Section 49 The Authority is a body tasked with the extremely important function of creating and ensuring an ecosystem of responsible data handling.[36] The Justice Srikrishna Committee Report (2018) further classified the functions of the Authority into these four categories: (1) monitoring and enforcement; (2) legal affairs, policy and standard setting; (3) research and awareness; and (4) inquiries, grievance handling and adjudication.[37] In essence, the Authority is the main regulatory body in the area of personal data, whether it be the stage of collection, processing or handling. Given the sensitive nature of data processing and data protection, and the rights of people that are in question, it is acknowledged that independence and transparency in the structure and functioning of the Authority are absolutely essential. To that end, we recommend the insertion of the text below tasking the Authority to ensure transparency in the exercise of its power and discharge of its functions.	
Proposed Text in Bill Section 49 Powers and functions of Authority.	**Recommended Text** Section 49 **(4) The Authority shall ensure transparency while exercising its power and discharging its functions through available means, including public consultations, wherever deemed fit.**

[36]Page 152 of the Srikrishna Committee Report.
[37]Page 153 of the Srikrishna Committee Report.

Rationale for the Recommendation

The recommended text is modelled around the transparency provisions in the establishing legislation of two other sectoral regulators, namely, the Telecom Regulatory Authority of India[38] and the Airports Economic Regulatory Authority of India.[39] The provision ensures that the ideal of transparency in the exercise of the Authority's functions and powers is specifically noted in the Bill.

The recommended text also provides for the modality of such transparency, noting that it can be done through public consultations, wherever the Authority deems it fit. Such public consultations contribute towards ensuring that decisions made by sectoral regulators are informed and democratic. (The importance and impact of public consultations on TRAI decisions was demonstrated during the Net Neutrality debate.)

[38]Section 11(2), Telecom Regulatory Authority of India Act, 1997.
[39]Section 13(4), Airports Economic Regulatory Authority of India Act, 2008.

10. On social media intermediaries and voluntary verification

10a. Comments on Section 26 and Section 28

Comments on Section 26 and Section 28 The effect that social media platforms have had on democracy and public order cannot be understated. The ease of dissemination of information has been revolutionised through the platform layer of the internet, with the proliferation of the use of social media platforms. Simultaneously, bad actors have hacked the human tendency to share sensational misinformation, compounded by virality-maximising algorithms of platforms. It is therefore acknowledged that attention must be paid to the deleterious impacts of misinformation and disinformation spread through these platforms. The ability of users to verify themselves on these websites could combat fake news to some extent, especially the kind which relies on misrepresentation and impersonation - assuming there is widespread awareness of the visible markers of identity verification and to the extent that misinformation relies on people's credulity. There is a very limited function to be served by defining social media intermediaries under this Bill, which might impact the effects of content moderation laws/ intermediary guidelines that need to be issued. We would also caution against the use of terms like "user" and "online interaction" that are not easily amenable to definition. There is an urgent need for content moderation guidelines to be created that will be applicable on all social media intermediaries, regardless of user density or the significance of the intermediary's impact on democracy. In our recommendations on the Intermediary Guidelines Amendment, we proposed the possibility of introducing a content moderation regulation along the lines of the Brazilian Marco Civil da Internet[40]. But this is a separate exercise and is not to be fitted into the ambit of the PDP bill.	
Proposed Text in Bill Section 26 (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	**Recommended Text** **Delete Section 26(4) and Explanation** **Delete Section 28(3) and (4)**

[40]Brazil Passes Groundbreaking Internet Governance Bill, available at https://www.zdnet.com/article/brazil-passes-groundbreaking-internet-governance-bill/

fiduciary: 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,— (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. Section 28 (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. (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.	

Rationale for the Recommendation

It is recommended that defining social media intermediaries on the basis of terms such as “users” and “online interaction” should be avoided under this statute. Not only are the terms difficult to define, qualifying social media intermediaries by a threshold of minimum users emerges from an impartial understanding of the origins of disinformation. Therefore, we recommend the deletion of 26(4) and its explanation defining social media intermediaries.

The Bill treats this category of social media intermediaries exactly like significant data fiduciaries, with the exception of the requirement to enable voluntary verification of notified social media intermediaries or class of social media intermediaries. Such a verification provision does not materially affect personal data protection rights, and should therefore be avoided in this Bill. A requirement for data fiduciaries to enable voluntary verification of identity is better placed in a content regulation law, and not a personal data protection law. Therefore, Section 28 (3) and (4) are deleted.

11. On biometric data

11a. Comments on Section 92

Comments on Section 92

Biometric data is a special class of data which has been classified as sensitive personal data ("SPD"). SPD, as a subset of personal data, is subject to all conditions on the treatment of personal data with additional enhanced safeguards, such as requirement of explicit consent, localisation restrictions, etc. Biometric data assumes further importance in view of its widespread use in identification techniques by the State machinery in law enforcement and welfare delivery. Thus, it is necessary to assess the specific restriction carved out for biometric data in Section 92.

Fingerprints are considered to be biometric data under the PDP Bill and the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act") classifies it as core biometric information. While the restriction on the use of core biometric information and Aadhaar information is regulated by the Aadhaar Act, the PDP Bill envisages a concept of horizontal privacy such that biometric data can be processed by both private and public parties.

Proposed Text in Bill	**Recommended Text**
Section 92 No data fiduciary shall process such biometric data as may be notified by the Central Government, unless such processing is permitted by law.	Section 92 No data fiduciary shall process ~~such~~ biometric data ~~as~~ **unless such biometric data has been** ~~may be~~ notified by the Central Government~~, unless such processing is permitted by law.~~ **and is processed in accordance with the law.**

Rationale for the Recommendation

There was no discussion regarding carving out a specific provision for processing of biometric data and to that extent, it is difficult to understand the intent of the provision. This is because a data fiduciary could make use of biometric data using the safeguards provided for SPD. At the same time, the intended provision in the Bill enhances the statutory safeguard for the use of biometric data, even beyond the protection offered to SPD under the Bill. The current provision puts restriction on processing of biometric data in two ways:

1. It excludes certain types of biometric data from being processed by data fiduciaries if it has been notified by the Central Government and;

2. The excluded biometric data can be processed, if permitted by law.

This understanding gives rise to two concerns:

1. All biometric data is subject to being processed unless it is excluded by a notification issued by the Central Government. Such biometric data can also be processed without law (it would need to comply with the requirements of SPD under the Bill only).

2. The excluded biometric data can be processed if it is permitted by law. This does not explain the scope of such processing. It does not explain if the processing of biometric data would be restricted to the extent identified by the law. For example, Aadhaar Act specifically excludes storage of core biometric information, while 'processing' in the Bill 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.*

Thus, any law permitting the processing of notified biometric data must also lay down the limits of such processing.

It is suggested that the language used in the law should indicate an obligation on the Central Government to notify the biometric data which can be used and not couch it in negative terms. To that extent, the recommended text for the provision has been suitably modified to take care of the concerns expressed. Secondly, the law should also provide the manner in which such biometric data can be used. This reform is urgently needed to regulate use of facial recognition technologies, CCTV surveillance and use of fingerprints in public and private spheres etc.