The Centre for Internet and Society's comments and recommendations to the:

The Personal Data Protection Bill 2019

20 February, 2020

By **Amber Sinha, Elonnai Hickok, Pallavi Bedi, Shweta Mohandas, Tanaya Rajwade**

The Centre for Internet and Society, India

General Comments

1. Executive notification cannot abrogate fundamental rights

In 2017, the Supreme Court in *K.S. Puttaswamy v Union of India*[1] held the right to privacy to be a fundamental right. While this right is subject to reasonable restrictions, the restrictions have to meet a three fold requirement, namely (i) existence of a law; (ii) legitimate state aim; (iii) proportionality.

Under the 2018 Bill, the exemption to government agencies for processing of personal data from the provisions of the Bill in the '*interest of the security of the State*'[2] was subject to a law being passed by Parliament. However, under Clause 35 of the present Bill, the Central Government is merely required to pass a written order exempting the government agency from the provisions of the Bill.

Any restriction on the right to privacy will have to comply with the conditions prescribed in Puttaswamy I. An executive order issued by the central government authorising any agency of the government to process personal data does not satisfy the first requirement laid down by the Supreme Court in *Puttaswamy I* — as it is not a law passed by Parliament. The Supreme Court while deciding upon the validity of Aadhar in *K.S. Puttaswamy v Union of India*[3] noted that "*an executive notification does not satisfy the requirement of a valid law contemplated under Puttaswamy. A valid law in this case would mean a law passed by Parliament, which is just, fair and reasonable. Any encroachment upon the fundamental right cannot be sustained by an executive notification.*"

2. Exemptions under Clause 35 do not comply with the legitimacy and proportionality test

The lead judgement in Puttaswamy I while formulating the three fold test held that the restraint on privacy emanate from the procedural and content based mandate of Article 21.[4] The Supreme Court in *Maneka Gandhi v Union India*[5] had clearly established that "*mere prescription of some kind of procedure cannot ever meet the mandate of Article 21. The procedure prescribed by law has to be fair, just and reasonable, not fanciful, oppressive and arbitrary.*"[6]

---

[1] (2017) 10 SCC 641 ("Puttaswamy I").
[2] Clause 42(1) of the 2018 Bill states that "*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, and is in accordance with the procedure established by such law, made by Parliament and is necessary for, and proportionate to such interests being achieved.*"
[3] (2019) 1 SCC 1 ("Puttaswamy II")
[4] *Puttaswamy I, supra,* para 180.
[5] (1978) 1 SCC 248.
[6] Ibid para 48.

The existence of a law is the first requirement; the second requirement is that of 'legitimate state aim'. As per the lead judgement this requirement ensures that"*the nature and content of the law which imposes the restriction falls within the zone of reasonableness mandated by Article 14, which is a guarantee against arbitrary state action."*[7] It is established that for a provision which confers upon the executive or administrative authority discretionary powers to be regarded as non-arbitrary, the provision should lay down clear and specific guidelines for the executive to exercise the power.[8]

The third test to be complied with is that the restriction should be 'proportionate' i.e. the means that are adopted by the legislature are proportional to the object and needs sought to be fulfilled by the law. The Supreme Court in *Modern Dental College & Research Centre v State of Madhya Pradesh*[9] specified the components of proportionality standards:

i. A measure restricting a right must have a legitimate goal;
ii. It must be a suitable means of furthering this goal;
iii. There must not be any less restrictive, but equally effective alternative; and
iv. The measure must not have any disproportionate impact on the right holder

Clause 35 provides extensive grounds for the Central Government to exempt any agency from the requirements of the bill but does not specify the procedure to be followed by the agency while processing personal data under this provision. It merely states that the 'procedure, safeguards and oversight mechanism to be followed' will be prescribed in the rules.

The wide powers conferred on the central government without clearly specifying the procedure may be contrary to the three fold test laid down in Puttaswamy I, as it is difficult to ascertain whether a legitimate or proportionate objective is being fulfilled.[10]

[7] Puttaswamy I *supra* para 180.
[8] *State of W.B. v. Anwar Ali Sarkar,* 1952 SCR 284; *Satwant Singh Sawhney v A.P.O* AIR 1967 SC1836.
[9] (2016)7 SCC 353.
[10] Dvara Research "Initial Comments of Dvara Research dated 16 January 2020 on the Personal Data Protection Bill, 2019 introduced in Lok Sabha on 11 December 2019", January 2020, *https://www.dvara.com/blog/2020/01/17/our-initial-comments-on-the-personal-data-protection-bill-2019/* ("Dvara Research").

3. Limited powers of Data Protection Authority in comparison with the Central Government

In comparison with the last version of the Personal Data Protection Bill, 2018 prepared by the Committee of Experts led by Justice Srikrishna, we witness an abrogation of powers of the Data Protection Authority (Authority), to be created, in this Bill. The powers and functions that were originally intended to be performed by the Authority have now been allocated to the Central Government. For example:

i. In the 2018 Bill, the Authority had the power to notify further categories of sensitive personal data. Under the present Bill, the Central Government in consultation with the sectoral regulators has been conferred the power to do so.

ii. Under the 2018 Bill, the Authority had the sole power to determine and notify significant data fiduciaries, however, under the present Bill, the Central Government has in consultation with the Authority been given the power to notify social media intermediaries as significant data fiduciaries.

In order to govern data protection effectively, there is a need for a responsive market regulator with a strong mandate, ability to act swiftly, and resources. The political nature of personal data also requires that the governance of data, particularly the rule-making and adjudicatory functions performed by the Authority are independent of the Executive.

4. No clarity on data sandbox

The Bill contemplates a sandbox for "innovation in artificial intelligence, machine-learning or any other emerging technology in public interest." A Data Sandbox is a non-operational environment where the analyst can model and manipulate data inside the data management system. Data sandboxes have been envisioned as a secure area where only a copy of the company's or participant companies' data is located.[11] In essence, it refers to the scalable and creation platform which can be used to explore an enterprise's information sets. On the other hand, regulatory sandboxes are controlled environments where firms can introduce innovations to a limited customer base within a relaxed regulatory framework, after which they may be allowed entry into the larger market after meeting certain conditions. This purportedly encourages innovation through the lowering of entry barriers by protecting newer entrants from unnecessary and burdensome regulation. Regulatory sandboxes can be interpreted as a form of responsive regulation by governments that seek to encourage innovation – they allow selected companies to experiment with solutions within an environment that is relatively free of most of the cumbersome regulations that they would ordinarily be subject to, while still subject to some appropriate safeguards and regulatory

[11] "A Data Sandbox for Your Company", Terrific Data, last accessed on January 31, 2019, http://terrificdata.com/2016/12/02/3221/.

requirements. Sandboxes are regulatory tools which may be used to permit companies to innovate in the absence of heavy regulatory burdens. However, these ordinarily refer to burdens related to high barriers to entry (such as capital requirements for financial and banking companies), or regulatory costs. In this Bill, however, the relaxing of data protection provisions for data fiduciaries could lead to restrictions of the privacy of individuals. Limitations to fundamental rights on grounds of 'fostering innovation' is not a constitutional tenable position, and contradicts the primary objectives of a data protection law. As the government continues to explore frameworks for innovation, it will be important that it coordinates with sectoral regulators to ensure harmonization. For example, The RBI has established a sandbox for banking sector[12] and TRAI has explored setting up a sandbox for the Telecom sector.[13]

5. The primacy of 'harm' in the Bill ought to be reconsidered

While a harms based approach is necessary for data protection frameworks, such approaches should be restricted to the positive obligations, penal provisions and responsive regulation of the Authority. The Bill does not provide any guidance on either the interpretation of the term 'harm,'[14] or "significant harm"[15] or on the various activities covered within the definition of the term. Terms such as 'loss of reputation or humiliation' 'any discriminatory treatment' are a subjective standard and are open to varied interpretations. This ambiguity in the definition will make it difficult for the data principal to demonstrate harm and for the Authority to take necessary action as several provisions are based upon harm being caused or likely to be caused. This is particularly concerning as the Bill envisions a tiered approach to harms - "harm" and "significant harm".

Some of the significant provisions where 'harm' is a precondition for the provision to come into effect are —

i. **Clause 25:** Data Fiduciary is required to notify the Authority about the breach of personal data processed by the data fiduciary, if such breach **is likely to cause harm** to any data principal. The Authority after taking into account the severity of the harm that may be caused to the data principal

[12] https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=48550
[13]https://main.trai.gov.in/notifications/press-release/trai-releases-telecom-commercial-communication-customer-preference
[14] Clause 3(20): "harm" includes (i) bodily or mental injury; (ii) loss, distortion or theft of identity; (ii) 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 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.
[15] Clause 3(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."

will determine whether the data principal should be notified about the breach.

ii. **Clause 32 (2):** A data principal can file a complaint with the data fiduciary for a contravention of any of the provisions of the Act, **which has caused or is likely to cause 'harm'** to the data principal.

iii. **Clause 64 (1):** A data principal who **has suffered harm** as a result of any violation of the provision of the Act by a data fiduciary, has the right to seek compensation from the data fiduciary.

Clause 16 (5): The guardian data fiduciary is barred from profiling, tracking or undertaking targeted advertising directed at children and undertaking any other processing of personal data that can cause **significant harm** to the child.

6. Non personal data should be outside the scope of this Bill

Clause 91(1) states that the Act does not prevent the Central Government from framing a policy for the digital economy, in so far as such policy does not govern personal data. The Central Government can, in consultation with the Authority, direct any data fiduciary to provide any anonymised personal data or other non-personal data to enable better targeting of delivery of services or formulation of evidence based policies in any manner as may be prescribed.

It is concerning that the data protection bill has specifically carved out an exception for the Central Government to frame policies for the digital economy and seems to indicate that the government plans to freely use any and all anonymized and/or non-personal data that rests with any data fiduciary that falls under the ambit of the bill to support the digital economy including for its growth, security, integrity, and prevention of misuse. It is unclear how the government, in practice, will be able to compel organizations to share this data. Further, there is a lack of clarity on the contours of the definition of non-personal data and the Bill does not define the term. It is also unclear whether the Central Government can compel the data fiduciary to transfer/share all forms of non-personal data and the rights and obligations of the data fiduciaries and data principals over such forms of data. Anonymised data refers to data which has 'irreversibly' been converted into a form in which the data principal cannot be identified. However, as several instances have shown 'irreversible' anonymisation is not possible. In the United States, the home addresses of taxi drivers were uncovered and in Australia individual health records were mined from anonymised medical bills.[16]

In September 2019, the Ministry of Electronics and Information Technology, constituted an expert committee under the chairmanship of Kris Gopalkrishnan to

[16] Alex Hern "Anonymised data can never be totally anonymous, says study", July 23, 2019 https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds.

study various issues relating to non-personal data and to deliberate over a data governance framework for the regulation of such data.

The provision should be deleted and the scope of the bill should be limited to protection of personal data and to provide a framework for the protection of individual privacy. Until the report of the expert committee is published, the Central Government should not frame any law/regulation on the access and monetisation of non-personal/ anonymised data nor can they create a blanket provision allowing them to request such data from any data fiduciary that falls within the ambit of the bill. If the government wishes to use data resting with a data fiduciary; it must do so on a case to case basis and under formal and legal agreements with each data fiduciary.

7. Steps towards greater decentralisation of power

We propose the following steps towards greater decentralisation of powers and devolved jurisdiction —

i. **Creation of State Data Protection Authorities:** A single centralised body may not be the appropriate form of such a regulator. We propose that on the lines of central and state commissions under the Right to Information Act, 2005, state data protection authorities are set up which are in a position to respond to local complaints and exercise jurisdiction over entities within their territorial jurisdictions.

ii. **More involvement of industry bodies and civil society actors:** In order to lessen the burden on the data protection authorities it is necessary that there is active engagement with industry bodies, sectoral regulators and civil society bodies engaged in privacy research. Currently, the Bill provides for involvement of industry or trade association, association representing the interests of data principals, sectoral regulator or statutory Authority, or an departments or ministries of the Central or State Government in the formulation of codes of practice. However, it would be useful to also have a more active participation of industry associations and civil society bodies in activities such as promoting awareness among data fiduciaries of their obligations under this Act, promoting measures and undertaking research for innovation in the field of protection of personal data.

8. The Authority must be empowered to exercise responsive regulation

In a country like India, the challenge is to move rapidly from a state of little or no data protection law, and consequently an abysmal state of data privacy practices to a strong data protection regulation and a powerful regulator capable of enabling a state of robust data privacy practices. This requires a system of supportive mechanisms to the stakeholders in the data ecosystem, as well as

systemic measures which enable the proactive detection of breaches. Further, keeping in mind the limited regulatory capacity in India, there is a need for the Authority to make use of different kinds of inexpensive and innovative strategies.

We recommend the following additional powers for the Authority to be clearly spelt out in the Bill —

i. **Informal Guidance:** It would be useful for the Authority to set up a mechanism on the lines of the Security and Exchange Board of India (SEBI)'s Informal Guidance Scheme, which enables regulated entities to approach the Authority for non-binding advice on the position of law. Given that this is the first omnibus data protection law in India, and there is very little jurisprudence on the subject from India, it would be extremely useful for regulated entities to get guidance from the regulator.
ii. **Power to name and shame:** When a DPA makes public the names of organisations that have seriously contravened data protection legislation, this is a practice known as "naming and shaming." The UK ICO and other DPAs recognise the power of publicity, as evidenced by their willingness to co-operate with the media. The ICO does not simply post monetary penalty notices (MPNs or fines) on its websites for journalists to find, but frequently issues press releases, briefs journalists and uses social media. The ICO's publicity statement on communicating enforcement activities states that the "ICO aims to get media coverage for enforcement activities."
iii. **Undertakings:** The UK ICO has also leveraged the threats of fines into an alternative enforcement mechanism seeking contractual undertakings from data controllers to take certain remedial steps. Undertakings have significant advantages for the regulator. Since an undertaking is a more "co-operative"solution, it is less likely that a data controller will change it. An undertaking is simpler and easier to put in place. Furthermore, the Authority can put an undertaking in place quickly as opposed to legal proceedings which are longer.

9. No clear roadmap for the implementation of the Bill

The 2018 Bill had specified a roadmap for the different provisions of the Bill to come into effect from the date of the Act being notified.[17] It specifically stated the

[17] Clause 97 of the 2018 Bill states*"(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 of 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 date 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*

time period within which the Authority had to be established and the subsequent rules and regulations notified.

The present Bill does not specify any such blueprint; it does not provide any details on either when the Bill will be notified or the time period within which the Authority shall be established and specific rules and regulations notified. Considering that 25 provisions have been deferred to rules that have to be framed by the Central Government and a further 19 provisions have been deferred to the regulations to be notified by the Authority the absence and/or delayed notification of such rules and regulations will impact the effective functioning of the Bill.

The absence of any sunrise or sunset provision may disincentivise political or industrial will to support or enforce the provisions of the Bill. An example of such a lack of political will was the establishment of the Cyber Appellate Tribunal. The tribunal was established in 2006 to redress cyber fraud. However, it was virtually a defunct body from 2011 onwards when the last chairperson retired. It was eventually merged with the Telecom Dispute Settlement and Appellate Tribunal in 2017.

We recommend that Bill clearly lays out a time period for the implementation of the different provisions of the Bill, especially a time frame for the establishment of the Authority. This is important to give full and effective effect to the right of privacy of the individual. It is also important to ensure that individuals have an effective mechanism to enforce the right and seek recourse in case of any breach of obligations by the data fiduciaries.

For offences, we suggest a system of mail boxing where provisions and punishments are enforced in a staggered manner, for a period till the fiduciaries are aligned with the provisions of the Act. The Authority must ensure that data principals and fiduciaries have sufficient awareness of the provisions of this Bill before bringing the provisions for punishment are brought into force. This will allow the data fiduciaries to align their practices with the provisions of this new legislation and the Authority will also have time to define and determine certain provisions that the Bill has left the Authority to define. Additionally enforcing penalties for offences initially must be in a staggered process, combined with provisions such as warnings, in order to allow first time and mistaken offenders from paying a high price. This will relieve the fear of smaller companies and startups who might fear processing data for the fear of paying penalties for offences.

---

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; (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 provision of the Act shall come into force eighteen months from the notified date."

10. Lack of interoperability

In its current form, a number of the provisions in the Bill will make it difficult for India's framework to be interoperable with other frameworks globally and in the region. For example, differences between the draft Bill and the GDPR can be found in the grounds for processing, data localization frameworks, the framework for cross border transfers, definitions of sensitive personal data, inclusion of the undefined category of 'critical data', and the roles of the authority and the central government.

11. Legal Uncertainty

In its current structure, there are a number of provisions in the Bill that, when implemented, run the risk of creating an environment of legal uncertainty. These include: lack of definition of critical data, lack of clarity in the interpretation of the terms 'harm' and 'significant harm', ability of the government to define further categories of sensitive personal data, inclusion of requirements for 'social media intermediaries', inclusion of 'non-personal data', framing of the requirements for data transfers, bar on processing of certain forms of biometric data as defined by the Central Government, the functioning between a consent manager and another data fiduciary, the inclusion of an AI sandbox and the definition of state. To ensure the greatest amount of protection of individual privacy rights and the protection of personal data while also enabling innovation, it is important that any data protection framework is structured and drafted in a way to provide as much legal certainty as possible.

Section Wise Comments and Recommendations

CHAPTER I PRELIMINARY

The preamble to the present Bill states that it is 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 personal data.....***laying down norms for social media intermediary***, accountability of entities processing personal data.....*"

Comments:.The inclusion of 'norms for social media intermediary' in the introduction and subsequent provisions (Clause 26 which creates the category of social media intermediary and Clause 28 which allows for users of the services of a social media intermediary to voluntarily verify their accounts) of the Bill is out of scope of a data protection legislation and risks conflicting with provisions provided for intermediaries under Section 79[18] of the Information Technology Act, 2000.

Recommendations: We recommend that this category and relevant provisions be removed from the Bill.

Clause 3: Definitions

Clause 3 of the Bill provides definitions to the terms used in the Bill. Some of the definitions provided could be strengthened and some terms used in the Bill require defining. We have called these out below:

- **Clause 3(3): "Anonymisation"**

  Comments: The Bill defines anonymisation as "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, which meets the standards of irreversibility specified by the Authority.

  Recommendations: Despite making the standards more specific by adding 'standards of irreversibility' **we reiterate our earlier comment.** The definition of anonymisation needs to protect privacy while enabling scientific research and innovation. There are multiple ways this can be achieved. For example, the term "irreversible" from the definition of anonymisation can be removed, in order to make provisions for the advancement in technology and research. This would also account for the challenges that exist with anonymization and the ability to

[18] Section 79 (1) of the Information Technology Act states "*Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-section (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.*"

re-identify individuals, as has been called out by many experts including the Sri Krishna Committee. In
the current form, there are various exemptions tied to anonymised data, therefore, a high threshold is appropriate and may be applicable at a later stage if anonymisation procedures do in fact assure irreversibility in the future. Alternately, we can choose to borrow from the definition of anonymisation from the Brazilian data protection bill which defines anonymised data as "data related to a data subject who cannot be identified, considering the use of reasonable and available technical means at the time of the processing." Another approach could be to require anonymisation through aggregation and once aggregated, personal data would no longer be protected under the Act. Aggregated data falls within the ambit of anonymised data, but could still raise community privacy concerns and thus fair and reasonable processing obligations would still need to apply.

- **Clause 3(8): "Child"**

Comments: The Bill defines a child as "a person who has not completed eighteen years of age." It is estimated that globally, one in three Internet users is a child under the age of 18.[19] As per the UNICEF Report on the State of the Children in 2017 [20],persons between the ages of 15 to 24 are the most connected age group and that children are increasingly accessing the internet at a younger age.; in some countries children under 15 are as likely to use the internet as adults over 25. The White Paper published by the Justice Srikrishna Committee[21] recognised the fact that a substantial percentage of internet users in India are children below the age of 18 and so prescribing 18 as the age below which children would necessarily require parental consent would not be feasible and may actually have a chilling effect on the child's opportunity to freely use the Internet as a medium of self-expression, growth and education.

In this regard, **we reiterate our previous comments**: The Srikrishna report justifies making the age of consent the same as that of contract by stating that the provision of consent for data sharing is often intertwined with consent to contract. However while stating about the non consensual processing of data the report

[19] Sonia Livingstone *et al*, "One in Three: Internet Governance and Children's Rights", G*lobal Commission on Internet Governance Paper Series No. 22* (November 2015) https://www.cigionline.org/sites/default/files/no22_2.pdf

[20] UNICEF, "State of the World's Children-Children in a Digital World", (2017) https://www.unicef.org/publications/index_101992.html

[21] White Paper of the Committee of Experts on a Data Protection Framework for India (2017) (SrikrihnaReport)https://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf

justifies it by stating that the relationship between a person and the state cannot be reduced to a contract. It is also important to note that in case of non consensual processing the report and the Bill is silent of the status of non consensual processing of the data of children.

Recommendations: We reiterate our previous recommendations: The provisions of parental consent allows the data fiduciary to implement services that will be used by children without ensuring that the data of children are processed with care. Such a responsibility should be reflected in the definition and under the 'privacy by design' principle found under chapter VII section 29. This would also provide children and parents with stronger grounds for redress- which are currently limited to the existence of consent. With this obligation in place, the age of mandatory consent could be reduced and the data fiduciary could have an added responsibility of informing the children in the simplest manner how their data will be used. Such an approach places a responsibility on data fiduciaires when implementing services that will be used by children and allows the children to be aware of data processing, when they are interacting with technology.

- **Clause 3(18): "financial data"**

Comments: We reiterate our previous comments: This definition is restrictive in its scope including only a) number or other personal data used to identify an account, card or payment instrument; b) personal data regarding the relationship between a financial institution and a data principal including financial status and credit history.

Recommendations*:* We reiterate our previous recommendations: The inclusive list in the second leg of the definition be expanded to include"financial statements, financial transactions and use of financial services offered by the financial institutions." We further recommend that the definition, without limitation, bring under its scope or refer to existing definitions of financial information such as that found in the "Master Direction Non-Banking Financial Company Account Aggregator (Reserve Bank) Directions, 2016" as it is connected to personal data."

- **Clause 3(28): "personal data"**

Comments: Though this definition has been expanded from the definition specified in the 2018 Bill to include*"and shall include any inference drawn from such data for the purpose of profiling"*,**we reiterate our previous comment:** 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. The phrase 'having regard to any characteristic, trait, attribute or any other feature of the identity of

such natural person' qualifies the scope of data to be classified as personal data. Therefore, data through which a natural person may be identified or identifiable but does not relate to any characteristic, trait, attribute or any other feature of the identity of such personal would not be covered under this definition. This would exclude information like identity numbers or other identifiers as long as they are not in combination with features of the identity of a natural person. Identifiers and pseudo-identifiers can be used to track individuals and in doing so can reveal identifying information. Thus, identifiers and pseudo-identifiers should be covered by the definition. Further, there is a lack of clarity about the terms 'identified' and 'identifiable'. The Article 29 Working Party in the EU has made recommendations in this regard, which we find to be appropriate. "A natural person can be considered as "identified" when, within a group of persons, he or she is distinguished from all other members of the group. A natural person is "identifiable" when, although the person has not been identified yet, it is possible to do it by taking into account all the means likely reasonably to be used either by a data fiduciary or by any other person to identify the said person.

Recommendations: We reiterate our previous comments: The definition of "personal data" be expanded further to include identifiers meant to track natural persons. The current definition would not cover an identity number that is stored by a data fiduciary along with other non-identity information. While identity numbers would get covered by this definition at the point at which the identity number is combined with "any characteristic, trait, attribute, or any other feature of the identity of such natural person", since identity numbers are also "other information", it is important for persistent identifiers to be treated differently from other forms of information. It would also be useful to clarify that "any aspect" of the identity of the person is covered by the definition. We further recommend that the definition of personal data in the Bill reflects the understanding of 'identified' and identifiable' as articulated by the Article 29 Working Party.

We suggest the following alternate definition of personal data:"*Personal data is 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 any aspect of the identity of such natural person, any identifiers intended to be associated with such natural person, any combination of such features or identifiers, or any combination of such features or identifiers with any other information.*"

- Terms that the Bill does not define or leaves for further defining by the Central Government or the Authority include:
    - Data Trust Score
    - Critical Personal Data
    - Employer/Employee
    - Non-personal data

  These should be clearly defined.

Chapter II - Obligations of Data Fiduciary

- **Clause 5: Limitation on purpose of processing of personal data:**

  Comments: The present Bill has removed language of any person processing personal data having a duty[22] towards data principals to process their data in a fair and reasonable manner and instead holds that "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."

  Recommendations: In our previous comments we had supported using the framing of a 'duty' and had recommended that in order to make the import of this provision clearer and in order to align it with the intent of protecting against harm as explained in the Report and incorporated through the Bill, we believe that adding the word fiduciary will make it clear that it means processing in the interest of the data principal. We suggest the following alternate language**:**
  "*Any person processing personal data owes a fiduciary duty to the data principal to process such personal data in a fair and reasonable manner that respects the privacy and does not harm the interests of the data principal.*"

Clause 5(b): Purpose limitation

Comments: This provision has not been changed from the 2018 Bill and we **reiterate our previous recommendations:** The Bill provides guidance on the standards of 'clear', 'specific' and 'lawful' and that further the Authority has a responsibility to publish and provide guidance on the standards of 'clear', 'specific', and 'lawful' as clearer definition evolve through use cases the Authority evaluates in it functioning. For example: A purpose is specific if it is detailed enough to determine what kind of processing is and is not included within the specific purpose. Purposes such as "improving users' experience", "marketing purposes", "IT-security purposes' " or "future research" will - without more detail - usually not meet the criteria of being 'specific'. A purpose is clear if it is expressed in such a way so as to be understood in the same way not only by the fiduciary (including all relevant staff) and any third party processors, but also by the data protection authority and the data principals concerned. The incidental purpose condition of this section should be replaced with the compatible purpose standard where the processing is compatible with the purposes for which the personal data was initially collected. In order to reduce function creep the processing of data must be similar to the purpose for which it was collected.

[22] Clause 4 of the 2018 Bill states "*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.*"

We further recommend that the assessment of compatibility be made on the basis of the following factors: (a) the relationship between the purposes for which the data have been collected and the purposes of further processing; (b) the context in which the data have been collected and the reasonable expectations of the data principals as to their further use; (c) the nature of the data and the impact of the further processing on the data principals; and (d) the safeguards applied by the data fiduciary to ensure fair and reasonable processing and to prevent any harm to the data subjects.

- **Clause 6: Collection Limitation**

Comments: This provision has not been changed from the 2018 Bill and we **reiterate our previous recommendations:** The test of proportionality should also be added under this clause such that it reads as follows: The collection of personal data shall be limited to such data that is necessary and proportionate for the purposes of processing.

- **Clause 7: Requirement of notice for collection or processing of personal data**

Comments: The provision specified under clause 7(1) is substantially similar to the provisions in the 2018 Bill. However, the exceptions to the requirement of providing notice have been expanded. Under the 2018 Bill[23], the data fiduciaries were not required to provide notice in two circumstances, namely in situations identified as requiring prompt action under clause 15 and 21 including medical emergency, provision of services during a threat to public health, and provision of services during a disaster or breakdown of public order. Under the present Bill, it has been expanded to include the exemptions under clause 12 to include when the data is processed for the provision of any service from the State, the issuance of any certification or licence by the State, under any law made by Parliament, and for compliance with any order or judgement of any court.

Recommendations: The exception to providing notice should be limited to the provisions specified in the 2018 Bill. In addition, **we reiterate our previous comments**: The provision of notice provides the data principal the right to be notified in order for her to provide informed consent. The notice should be transparent and must inform the data principal of not only her rights but also of the duties of the data fiduciary. Clause 12(4) of this Bill states that if the data principal withdraws her consent for the processing of any personal data necessary for the performance of a contract to which the data principal is a party, then all legal consequences of the effects of such withdrawal shall be borne by the data

[23] Clause 11(3) of the 2018 Bill states "*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 Section 15 or 21 of this Act*"

principal. Hence the notice should also communicate to the data principal the nature of the relationship between the two, and whether there is a statutory or contractual requirement. Additionally, the notice should communicate the possible consequences when she fails to provide such data, as well as withdrawal from processing. This is similar to Article 13(2)(e) of the GDPR. The data principal must also have the right to know if her data is being used to make automated decisions about her. The Report of the DP Bill justifies the absence of this right by stating that the Bill already has a provision to seek legal recourse in case of harm or a breach. However, we recommend that it is important to include this provision so that this remedy can be directly claimed from the data fiduciary without putting additional burden on the Authority. The data principal must be informed of the existence of automated decision making including profiling (as defined under Section 2(33) of this Bill).

- **Clause 11: Consent necessary for processing of personal data**

Comments: The clause is substantially similar to the provisions in the 2018 Bill and **we reiterate our previous comments:** This clause states that consent needs to be sought no later than at the commencement of processing, however it might be difficult for a data principal to assess at the commencement of the processing in which all ways the data will be processed in the future. As the use of data to provide services becomes more pervasive and connected to other services the data might be processed by the fiduciary in ways that the data subject had not consented for. Clause 30(2) states that the data fiduciary shall notify the data principal of important operations in the processing of personal data through periodic notifications. However this provisions do not speak about seeking consent from the data principal for the new processing.

The system of blanket consent is problematic as it takes away the autonomy from the data principal. The report of the Data Protection Bill proposes the formation of consent dashboards in order to reduce consent fatigue and to provide the data principal with information and autonomy over their data. The report also states that the dashboard would provide a system where the data fiduciary will be notified and consent be sought a new in the case of a processing that she had not consented to. However, the consent dashboard will be a time consuming process not only to implement but also to educate the data principals of its usage. Hence the Bill should provide minimum safeguards and measures to ensure that the data principal has autonomy over her data, and mere notice does not serve the purpose. The provision for withdrawal of consent can be justified as a reason, however if the principal wants to use the service offered by the data fiduciary but objects to the recent addition of processing she has only two options one to agree to the processing and two to withdraw from the service altogether.

Recommendations: We reiterate our previous comments: Clause 12 could state that the consent needs to be sought not just at the commencement of the

processing but also at instances where the personal data is being processed for a purpose that was not stated at the time of consent. The report of the PDP Bill states about the importance of reducing consent fatigue however the choice needs to be on the data principal to know and consent to each new processing. The data principal must be allowed to enjoy the services for which she had consented for and given the choice to not consent for some processing that is not directly related to the service.

Chapter III-GROUNDS FOR PROCESSING OF PERSONAL DATA WITHOUT CONSENT

General Recommendation:
At the outset, **we reiterate our previous comment:** necessity and proportionality need to be the two conditions that are imperative for non consensual data protection. We suggest the following alternative language for all the provisions that deals with non consensual processing in the Bill "*Personal data maybe processed if such processing is necessary and proportionate.*"

- **Clause 12: Grounds for processing of personal data without consent in certain cases**

Comments: Clause 12 (a) provides that 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) for the issuance of any certification, license or permit for any action or activity of the data principal by the State.

Recommendations: The provision of any and all public services or benefits should not be a blanket exemption to the consent requirement. Guidelines could be provided for the Authority/Central Government to identify and notify the specific delivery of public services permitting non-consensual processing of personal data of the data principal.

In addition, **we reiterate our previous comment:** the conditions for non-consensual processing of personal data should rely not only on necessity, but also on proportionality. The Puttaswamy judgement laid out the three pronged test of necessity, legitimacy and proportionality. The non- consensual use of data by the state for providing services for the benefit of the data principal needs to be not just necessary but also proportional to the exercise of the function of the state.

Comments: Clauses 12 (b) to (f) provides that personal data may be processed if such processing is necessary:

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

(c) for compliance with any order or judgement of any Court or Tribunal in India;
(d) to respond to any medical emergency involving a threat to the life or a severe threat to the health of the data principal or any other individual;
(e) to undertake any measure to provide medical treatment or health services to any individual during an epidemic, outbreak of disease or any other threat to public health; and
(f) to undertake any measure to ensure the safety of, or provide assistance or services to any individual during any disaster or any breakdown of public order.

Clause 13 and 14 of the 2018 Bill providing for non-consensual processing of personal data have been condensed into Clause 12 (b) and (c) of this Bill. However, by virtue of Clauses 12 (c) to (f) it has also included the grounds for non-consensual processing of sensitive personal data provided under the 2018 Bill under the ambit of this clause. Under the 2018 Bill, the corresponding provisions for processing of sensitive personal data required compliance with a higher threshold. For instance, processing of sensitive personal data for prompt action[24] and for certain functions of the State[25] had to be *strictly necessary* and similarly, processing of sensitive personal data in compliance with law or any order of any court could be undertaken if such processing is *explicitly mandated* under any law made by Parliament or any State Legislature or is *necessary* for compliance with any order or judgement of any court or tribunal.

Recommendations: The grounds for processing of sensitive personal data without consent and personal data without consent should be separately enumerated. Further, **we reiterate our previous comment**: for the processing of sensitive personal data for the functions of the state the test of necessity is, by itself not enough and needs to be strengthened with the principle of proportionality.

- **Clause 13: Processing of personal data necessary for purposes related to employment etc.**

Comments: We appreciate that this clause now requires consent for the processing of sensitive personal data by employers. However, it is unclear on what basis and by whom a determination will be reached where the consent of the data principal

[24] Clause 21 of the 2018 Bill states "*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 life 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;(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.*"
[25] Clause 19 of the 2018 Bill states "*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.*

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 processing. Furthermore, the Bill does not define the term employment or employee nor does it refer to a specific definition in Indian law; leaving it unclear if the provisions will extend to all forms of work and types of people in the workforce.

- **Clause 14: Processing of personal data for other reasonable purposes**

  Clause 14 establishes eight purposes for which personal data may be processed without consent: prevention and detection of any unlawful activity including fraud, whistle blowing, mergers and acquisitions, network and information security, credit scoring, recovery of debt, processing of publicly available personal data, and operation of search engines. The list has been expanded from the 2018 Bill to include operation of search engines.

  For this, the processing must be necessary and the decision must be weighed against 5 considerations. The authority will also determine if notice under clause 7 is applicable or not.

  Comment and Recommendation: We recommend that the provision requires that processing of personal information without consent must be both **necessary** and **proportionate**. Furthermore, we recommend that 'credit scoring' and 'the operation of search engines' are removed from the list of purposes that may constitute 'reasonable purposes'. We also recommend removing 'prevention and detection of any unlawful activity including fraud' as we believe it is covered under the exception carved out in clause 36 (a). We finally recommend that standards be defined on which the authority makes a determination regarding the applicability of clause 7 (notice).

- **Clause 15: Categorisation of personal data as sensitive personal data**

  Comments: This clause has been changed to empower the Central Government, in consultation with the Authority and the concerned sectoral regulators to notify further categories of personal data as sensitive personal data on the basis of four specified criteria. Under the 2018 Bill,[26] the Authority had the sole authority to classify further categorise personal data as sensitive personal data.

  Recommendations: The rationale for authorising the Central Government, albeit in consultation with the Authority and the sectoral regulator to notify categories of

[26] Clause 22 (1) of the 2018 Bill states"*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.*"

personal data as sensitive personal data is unclear. We recommend that the provision as per the 2018 Bill should be reinstated and the Authority in consultation with the sectoral regulators should be empowered to determine further categories of personal data.

CHAPTER IV PERSONAL DATA AND SENSITIVE PERSONAL DATA OF CHILDREN

- **Clause 16-Processing of personal data and sensitive personal data of children**

Comments: The clause provides that every data fiduciary shall process the personal data of a child in such a manner that is in the best interest of, and protects the right of the child. It further provides that the data fiduciary shall before processing the personal data of any child, verify his age and obtain the consent of the parent or the guardian. However, there is no provision for the data principal to withdraw her consent upon attaining the age of majority. In July 2019, the Central Government amended the Aadhar Act[27] permitting a child who has been enrolled in the Aadhar database by her parents/guardian to seek cancellation of her Aadhar within six months of her attaining the age of 18.

Recommendations: We recommend that upon attaining the age of majority, the data principal should have the right to withdraw her consent to any further processing of her data. Further, **we reiterate our earlier recommendation:** The data principal on attaining majority (according to the Act) has the right to be informed about the personal data that has been collected of her. However as this would require the collection of data about the age of the child there needs to be added protection with respect to this data including additional safeguards to prevent the data being used for further processing and profiling. Additionally the data fiduciary should seek consent anew from the data principal on attaining majority and the data principal should have the right to withdraw from the processing if she chooses not to consent to further processing.

CHAPTER V- RIGHTS OF DATA PRINCIPAL

- **Clause 17: Right to confirmation and access**

Comments: Under the 2018 Bill, the data principal had the right to obtain a brief summary of the personal data that had been processed or was being processed. This has now been amended to permit the data principal to access the actual personal data that has been processed. Further, it now also permits the data

[27] Insertion of Section 3A to the Aadhaar (Targeted Delivery of Financial and Other Subsidies,Benefits and Services) Act, 2016 by virtue of Aadhaar and other Laws Amendment Act, 2019.

principal to have the right to access in one place the identities of the data fiduciaries with whom the data has been processed along with the categories of the personal data shared with them.

Recommendations: We appreciate the expanded right to access provided to the data fiduciary, however **we would also reiterate our previous comment:** It is also imperative that along with the right to confirmation, the data principals are also provided information justifying the ground under which the processing is being conducted. Further, we recommend the addition of sub clause (c) which states as follows: *"an explanation of how the processing is justified under one or more of the provisions under Chapters III and IV*."

- **Clause 19: Right to data portability**

Comments: Clause 19(1) provides that where the processing has been carried out through **automated** means, the data principal shall have the right to receive the data in a structured, commonly used machine- readable format. This provision has been changed from the 2018 Bill where this right applied to all data and not only data processed through automated means.

Recommendations: We recommend that this right be applicable to all data and should not be limited to data processed through automated means.

- **Clause 20: Right to be forgotten**

Comments: There is no substantive change in this provision from the 2018 Bill and **we reiterate our previous comments:** The provision seems to be misnamed as the Bill does not provide a right to be forgotten, but instead a right to restrict processing.

Recommendations: We reiterate our previous recommendations:

1. This Clause''s heading could be changed from "Right to be Forgotten" to "Right to Prevent Continuing Disclosures" and should include a right for the individual to request that information pertaining to them is de-indexed.

2. The Bill also empowers an adjudicating officer for the acceptance of complaints and making the decision. The report of the data protection Bill justifies making a central adjudicating authority as the approving entity instead of the data fiduciary in order to prevent privatisation of regulation. However a singular authority to approve requests, to adjudicate over them puts a heavy burden on this authority that might not have the capacity to handle the flow of requests that will be coming in. Additionally, the authority will have to coordinate with the data fiduciary for each request

making the process severely time consuming. With respect to personal data and sensitive personal data this can be crucial. The data fiduciary could be given the authority to erase the data based on the data principal's complaints, the data principal could also be accountable to an adjudicating authority including providing an account and reasoning for requesting each erasure and the reason thereof.

General Comments: While we appreciate that the Bill has provided the data principal the right to seek erasure of personal data, we also **reiterate our previous recommendation:**

(a) Right to restriction of processing

The data principal shall have the right to obtain from the data fiduciary restriction of processing where one of the following applies:

(1) the accuracy of the personal data is contested by the data principal, for a period enabling the fiduciary to verify the accuracy of the personal data:

(2) the processing is unlawful and the data principal opposes the deletion of the personal data and requests the restriction of their use instead; or

(3) the fiduciary 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 defence of legal claims.

(b) Right to object to processing

The data principal shall have the right to object to processing at any time being carried out under Clause 13, Clause 17 and Clause 19. Upon such objection, the fiduciary shall immediately stop processing the personal data unless they can demonstrate compelling grounds for processing for the establishment, exercise or defence of legal claims.

CHAPTER VI- TRANSPARENCY AND ACCOUNTABILITY MEASURES

- **Clause 22: Privacy by design policy**

Comments: The provision is similar to the provision in the 2018 Bill and **we reiterate our previous comments:** the Bill should not only emphasise on privacy by design but also on privacy by default. The Bill could ideally also add these following policy measures to ensure purpose limitation and data minimisation.

1. The data fiduciary shall implement measures to ensure that only that personal is collected which is necessary for and proportional to each specific purpose of the processing.

2. The data fiduciary especially those that process sensitive personal data must practice data minimisation, and implement measures such as anonymisation.

Further, though it is welcome that the Bill requires that the privacy by design policy of each data fiduciary should be published on their website as well as the website of the Authority; this provision could be strengthened by creating a timeframe after certification by which the policy needs to be published and requiring that the policy is updated and re-certified if and when significant changes are made to the way in which personal data is handled.

- **Clause 23: Transparency in processing of personal data**

Comments: There has been a change in the wording from the 2018 Bill[28]. In the present Bill, the term "available in an easily accessible form" has been replaced with ***"information available in such form and manner as may be specified by regulations."***

Recommendations: The need to maintain some level of transparency by the data fiduciary is essential to allow the data principal to assert their rights provided by the Bill. Reports on the privacy policies of companies have provided how length and legalese make these essential policies inaccessible to individual users.[29] Hence we suggest that the earlier wording of the 2018 version be restored to ensure that the data principal is aware of the rights that they are entitled to.

Consent Manager: Clause 23(3) creates the role of a 'consent manager'. It 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." The Authority has the power to define the technical, operational, financial, and other conditions of the consent manager via regulation. Though the role of a 'consent manager' can be an important intermediary structure in enabling

[28] Clause 30(1) of the 2018 Bill states that "*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.*"
[29] Rishabh Bailey et al "Disclosures in privacy policies: Does "notice and consent work? ", NIPFP Working paper series (2018), https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf, Aayush Rathi and Shweta Mohandas, "FinTech in India, A study of privacy and security commitments", (April 2019), https://cis-india.org/internet-governance/files/Hewlett%20A%20study%20of%20FinTech%20companies%20and%20their%20privacy%20policies.pdf/view

individuals to provide meaningful consent, the current structure in the Bill is ambiguous and does not answer important questions about the functioning of a consent manager.

- **Clause 24: Security safeguards:**

  This clause requires data fiduciaries to develop security safeguards based on the associated risks and the likelihood and severity of harm including de-identification and encryption, steps to protect the integrity of data, and steps to prevent misuse, unauthorised access, and modification and disclosure/destruction of personal data. These practices need to be reviewed periodically in a manner specified by regulations. Though, it is welcome that the Bill includes provisions around security, given the importance of security in the digital age, there is no clear form of accountability or baseline standard for security. This could result in a vast range of security practices emerging in India and levels of enforcement and could overall weaken national cyber security.

  Recommendation: We recommend that the text of the Bill require an annual review rather than a periodic review and require that the review involve an audit by an independent third party. The results of such an audit should be included in the data trust score that is assigned to a data fiduciary. We further recommend that the Bill require adherence to security standards that have been recognized and approved at the sectoral, national, or international level.

- **Clause 25: Reporting of personal data breach**

  Comments: The provision is similar to the provision specified the 2018 Bill and **we reiterate our previous comments**:

  (a) The fiduciary must report the breach as soon as possible and no later than the time period specified by the Authority. It does not indicate what a reasonable time period may look like. Further, the responsibility to determine this time period is not included under 'Powers and Functions of the Authority' which have been charted out under clause 60. Note under the present Bill also the responsibility to determine the time period has not been included under the Powers and Functions of the Authority specified under Clause 49. It has also not been included under Clause 94; which provides the matters on which the Authority is empowered to make regulations.

  (b) Section 32(5) states that the Authority may choose to compel the fiduciary to report the breach to the data principal depending on the severity of the breach, the harm likely to be caused to the data principal and any mitigating action the data principal may need to take. The Bill does not

provide any clarification on the meanings or the thresholds envisaged by these terms and places absolute discretion on the Authority to determine whether the data principal should be made aware of a breach of his/her personal data. This is potentially problematic for two reasons. First, informing the data principal enables the individual to take context specific measures that would remedy the harms caused by the breach in his/her specific situation-something the Authority may be ill-equipped to determine. Second, from an insurance industry perspective,if breaches are not reported, customers will not be concerned about cyber risk and therefore will be less inclined to buy insurance.

Recommendations: We reiterate our previous recommendations:

- Impose a reasonable time limit on the data fiduciary to report data breaches under clause 32(3) or empower the Authority to decide time limits under clause 60.
- Instead of enabling the Authority to decide when to notify the breach to the data principal, amend clause 32 (5) to make this disclosure mandatory. The Authority should be allowed to withhold this information only in the case of narrowly defined exceptions such as national security.

- **Clause 26 (4) and Clause 28 (3): Classification of data fiduciaries as significant data fiduciaries**

Comments: Clause 26 (4) empowers the Central Government in consultation with the Authority notify any social media intermediary as a significant social data fiduciary if (a) the social media intermediary has users above the threshold notified by the Central Government; and (b) the activities of the intermediary 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**.

Clause 28 (3) further states that every social media intermediary which has been notified as a significant data fiduciary shall enable the users who register their services from India, or use their services in India, to voluntarily verify their accounts.

As mentioned in the General Comments, the classification of social media intermediaries and the verification obligation are out of the scope of a data protection legislation. Additionally, the construct of social media intermediaries as significant data fiduciaries suffers from several issues:

(a) With respect to the conditions for social media intermediaries to be designated under clause 26, the numerical thresholds are to be set with respect to the number of 'users'. The term 'user' has not been defined in the Bill or elsewhere in this context, and the Bill is silent on the treatment

given to non-registered users or the level of activity required to be counted as a user.

(b) The condition requiring assessment for 'significant impact on electoral democracy' is vague, which may incentivise social media intermediaries to implement overly-restrictive content moderation practices to avoid designation.

(c) The Authority, which has been tasked with notifying significant data fiduciaries in all other cases, has been relegated to a consultative role with respect to social media intermediaries. The rationale behind this differential treatment is not clear.

(d) Regulation relating to voluntary verification of users is the subject matter of delegated legislation. The rules notified in this regard may dilute the 'voluntary' nature of verification, given the lack of a guiding framework in the parent Bill.

Recommendations: Provisions relating to social media intermediaries and the verification of the user's accounts should be deleted from the Bill.

- **Clause 32: Grievance redressal by data fiduciary**

Comments: The clause is substantially similar to the provisions in the 2018 Bill. The provision while laying out the process for grievance redressal and the measures that are needed to be taken by the data fiduciary, does not lay out the mechanisms through which the grievance can be made.

Recommendations: **We reiterate our earlier recommendations**: We suggest the inclusion of a list of key mechanisms to be added to this clause and we suggest the following alternate language:"*The data principal may raise a grievance through online lodging, toll-free calling lines, e-mail, letter, fax or in person to the Data Protection Authority.*"

CHAPTER VII-RESTRICTIONS ON TRANSFER OF PERSONAL DATA OUTSIDE INDIA

- **Clause 33: Prohibition on processing of sensitive personal and critical personal data outside India**

Comments: This provision has changed from the 2018 Bill.[30] Instead of requiring the storage of one serving copy of personal data within India and a strict limitation on critical personal data and sensitive data, there is now no restriction on the transferring of personal data outside of India. However, sensitive personal data shall continue to be stored in India and critical personal data can only be processed in India. Though it is a welcome change that personal data can be transferred outside of India, we maintain our concerns with the government applying a 'one size fits all' data localization requirements in a data protection bill and would encourage the government to consider sectoral regulation around specific categories of data such as defense related data. We are also concerned with the creation of the undefined category of 'critical personal data' as it creates an uncertain environment for companies to operate in and could lead to enforcement and implementation issues if the category is frequently changed.

Recommendation: We recommend that this provision as well as the category of 'critical data' are removed from the Bill.

- **Clause 34: Conditions for transfer of sensitive personal data and critical personal data.**

Comments: Sensitive personal data can be transferred outside of India as per the conditions specified under this clause including if the transfer is pursuant to an approved contract or intra-group scheme or the Central Government allows such transfer. Critical personal data can be transferred outside India to an entity engaged in the provision of health services or emergency or where the Central Government has deemed the transfer permissible. This is a change from the 2018 Bill[31] which allowed for the transfer of personal data outside of India based on five conditions and only permitted the transfer of sensitive personal data outside India on two conditions while maintaining that critical personal data could only be processed in India.

---

[30] Clause 40 of the 2018 Bill states "(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 a data center 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."*

[31] Clause 41(3) of the 2018 Bill states "*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 transfer is necessary for any class of data fiduciaries or data principals and does not hamper the effective enforcement of this Act.*"

Recommendation: We recommend the following with respect to this provision:

- It is assumed that the intra-group schemes referred to in this section are similar to the binding corporate rules found in the GDPR. Under the GDPR there are multiple tools for international data transfers including adequacy findings, binding corporate rules, explicit consent, standard contractual clauses, and approved codes of conduct/certification.[32] Clause 34 appears to combine different mechanisms (consent, contract, and intra-group scheme) into one mechanism - with the only other mechanism for transfer being approval by the Central Government. The Government should create a set of multiple comprehensive mechanisms by which sensitive data can be transferred outside of India.
- The Authority should be the sole entity responsible for assessing and approving such mechanisms.
- Personal data should be brought back into the scope of this provision as the current framing excludes personal data and thus would mean that it can be transferred outside of India without assurance that it is being processed inline with the requirements found in the Bill.
- The provision should clarify at a more granular level how each transfer mechanism will work and what criteria must be met for approval. For example, it is currently unclear if the provision will require each transfer to be approved by the government/authority or if the government/authority will approve an intra-group scheme - after which companies can transfer data freely.

Chapter VIII- EXEMPTIONS

General Comments: Under the 2018 Bill, exemptions were provided to the data fiduciary from the various provisions of the Bill in cases of processing of (i) personal data required for the security of the State, (ii) Prevention, investigation, prosecution and contravention of law, (iii) Processing for the purpose of legal proceedings, (iv) Research, archiving or statistical purposes, (v) personal and domestic purposes, and (vi) Manual Processing by small entities. However, any data fiduciary processing personal data for such specified purposes was still required to comply with the provision of fair and reasonable processing. Under the present Bill, similar grounds have been provided for exemptions from the various provisions of the Bill, but unlike the 2018 Bill, under the present Bill, the exemptions from the applicability of the provisions of the Bill has been expanded to include exemption from fair and reasonable processing of personal data.

In addition, **we also reiterate our earlier comments:**

32 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

(a) The standard of necessary and proportionate for the security of state, or prevention, detection, investigation and prosecution of contraventions of law is too vague. While it may not be possible to exhaustively define what constitutes as necessary and proportionate, it would be extremely useful to include explanations which provide guidance about how these legal tests ought to be construed.

(b) In its current formulation, there is no obligation and clear procedure for the agencies involved to establish necessity and proportionality before a judicial or quasi-judicial body. We recommend that a commission be set up by the Authority to examine all requests for processing under Clause 42 and 43 and be subject to their determination.

(c) We recommend that duration limitation, that is, data will only be retained for a given period and destroyed after that, be specified under Clause 42 and 43;

(d) Exemption under Clauses 42 and 43 need not be as sweeping as they have been drafted currently. Requirements such as reporting personal data breaches to the Authority and data audits should continue to apply;

(e) We also recommend that user notifications rights be made available under both Clause 42 and 43. Such notification maybe withheld as long as it cannot be ruled out that informing the data subject might jeopardise the purpose of the processing or as long as any general disadvantages to the interest of purposes under Clause 42 and 43.

(f) Similarly, a limited right to confirmation, access and rectification must be made available to data principals where their personal data is being processed under Clause 42 and 43. These rights maybe limited to the extent such conformation,access and rectification jeopardises the purpose of processing.

- **Clause 35: Power of the Central Government to exempt any agency of the Government from the application of the Act**

Comments: Under the 2018 Bill[33], the exemption was granted for the security of the State, subject to such processing of personal data being (i) authorised by law; (ii) in accordance with the procedure laid down by the law; (iii) necessary; and (iv) proportionate to the interests being achieved. This four stage process embed the principles laid down by the Supreme Court in Puttaswamy I. This was regarded as a first step towards determining the surveillance powers of the State, even though the other recommendation of the Srikrishna Committee regarding an *ex-ante* judicial approval of the process was not included in the Bill.

[33] Clause 42 (1) of the 2018 Bill states "*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, and is in accordance with the procedure established by such law, made by Parliament and is necessary for, and proportionate to, such interests being achieved.*"

However, under the present Bill, this four stage process has been done away with. The provision now merely provides that the Central Government if it is satisfied that it is **necessary or expedient** to do so may by a written order exempt any agency of the Government from the application of all or any of the provisions of this Bill in respect of the processing of such personal data **subject to such procedure, safeguards and oversight mechanism as may be prescribed**. Further, the grounds for such an exemption has been expanded to include processing for the sovereignty and integrity of India, security of the State, friendly relations and public order. These are the restrictions on freedom of speech and expression provided under Article 19(2) of the Indian Constitution which have now been provided as a measure to exempt protection of personal data.

The present Bill grants a blanket exemption from all the provisions of the Bill to an agency of the Central Government- it is not specific to a particular function or specific purpose of the particular agency. Unlike, the 2018 Bill[34], where the exemptions were granted from certain specific provisions, under the current Bill, power has been granted to exempt the agency from any or all the provisions of the Bill, thereby exempting it from the obligations specified under Chapter XIII (offences), Chapter X (Penalties and Compensation) , Chapter IX (Data Protection Authority of India).

By doing away with the four pronged test, these provisions are not in consonance with test laid down by the Supreme Court in and are also incompatible with an effective privacy regulation. There is also no provision for either a prior judicial review of the order by a district judge as envisaged by the Justice Srikrishna Committee Report or post facto review by an oversight committee of the order as laid down under the Indian Telegraph Rules, 1951[35] and the rules framed under Information Technology Act[36]. The provision states that such processing of

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

[35] Rule 419A (16): The Central Government or the State Government shall constitute a Review Committee.
Rule 419 A(17): The Review Committee shall meet at least once in two months and record its findings whether the directions issued under sub-rule (1) are in accordance with the provisions of sub-section (2) of Section 5 of the said Act. When the Review Committee is of the opinion that the directions are not in accordance with the provisions referred to above it may set aside the directions and orders for destruction of the copies of the intercepted message or class of messages.

[36] Rule 22 of Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009: The Review Committee shall meet at least once in two months and record its findings whether the directions issued under rule 3 are in accordance with the provisions of sub-section (2) of section 69 of the Act and where the Review Committee is of the opinion that the directions are not in accordance with the provisions referred to above, it may set aside the directions and issue an order for destruction of the copies, including corresponding electronic record of the intercepted or monitored or decrypted information.

personal data shall be subject to the procedure, safeguard and oversight mechanisms that may be prescribed. However, there is no corresponding provision under Clause 93, which grants powers to the Central Government to make rules on specified grounds.

Recommendations: In addition to the recommendations made under the General comments, we recommend the following:

- The exemption should be subject to the four stage test specified under the 2018 Bill. i.e. (i) authorised by law; (ii) in accordance with procedure established by such law; (iii) necessity; and (iv) proportionate.

- The procedure and the safeguards should be provided for in the parent Bill and not be delegated to the rules to be framed by the Central Government.

- The exemptions should not be as sweeping as have been provided for currently. There is no need for exemptions from the Chapter XIII (Offences), Chapter IX (Data Protection Authority of India), security safeguard measures. Requirements such as reporting personal data breaches to the Authority and data audits should continue to apply.

- Prior judicial review of the written order exempting the agency of the Central Government from the provisions of this Bill.

- **Clause 36: Exemptions of certain provisions for certain processing of personal data**

Comments: Clause 36 (a) provides for exemptions of certain provisions where the 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. Under the 2018 Bill[37], a condition precedent for this clause to come into effect was (a) a law made by Parliament or State Legislature authorising such exemptions and (b) it was necessary for and proportionate to the interests sought to be achieved. These requirements have been deleted from this Bill.

Further, under the 2018 Bill[38] such exemptions in relation to the processing of personal data would apply to a victim, witness or any person with information about the offence/contravention of law. This provision/requirement has also been

---

[37] Clause 43 (1) of the 2018 Bill states"*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 is necessary for, and proportionate to, such interests being achieved.*"

[38] Clause 43 (3) of the 2018 Bill states *"Sub-section (1) shall apply in relation to the 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.*"

deleted from this Bill. The 2018 Bill also stated that the personal data so processed shall not be retained once the purpose for which it was processed is competed[39]. This provision has also been deleted from this present Bill.

As per the current provision, personal data could be processed for the prevention, detection, prosecution of any offence. The term 'offence' has not been defined and therefore even a breach of a contractual provision could constitute an offence for the purposes of this provision.

Recommendations: In addition to the recommendations made under the General comments, we recommend the following:

- The personal data so processed should be deleted once the purpose for which it was processed under this clause has been completed.
- Re-introduction of provisions in the 2018 Bill specifying the persons to whom this provision would be applicable.
- Determining the scope of the term 'offence' to include only cognizable offences as defined under the Code of Criminal Procedure, 1973.

- **Clause 38: Exemptions for research, archiving or statistical purposes**

Comments: Under the 2018 Bill[40], the Authority could exempt a data fiduciary from the application of any provisions of the Bill in cases where the personal data is processed for research, archiving or statistical purposes. However, provisions regarding 'fair and reasonable processing', 'security safeguards' and 'data protection impact assessment' still had to be complied with. Under the 2019 Bill, the requirement for compliance with these provisions has been deleted.

Recommendations: The exemptions should be narrowed down and the provisions specified in the 2018 Bill should be reinstated.

- **Clause 40: Sandbox for encouraging innovation etc.**

[39] Clause 43 (4) of the 2018 Bill states "*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.*"
[40] Clause 45(1) of the 2018 Bill states "*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.*"

Comments: The Authority for the purpose of encouraging innovation in artificial intelligence, machine learning or any other emerging technology in public interest, will create a sandbox.

Any data fiduciary whose privacy by design policy is certified by the Authority can apply. The sandbox will involve relaxing requirements that obligate specification of purpose, limitation of personal data, restrictions on retention of personal data, and requirements for the processing of data in a fair and reasonable manner with consent. As mentioned in the General Comments, data sandboxes have been envisioned as a secure area where only a copy of the company's or participant companies' data is located.[41] In essence, it refers to the scalable and creation platform which can be used to explore an enterprise's information sets. On the other hand, regulatory sandboxes are controlled environments where firms can introduce innovations to a limited customer base within a relaxed regulatory framework, after which they may be allowed entry into the larger market after meeting certain conditions.

Sandboxes are regulatory tools which may be used to permit companies to innovate in the absence of heavy regulatory burdens. However, these ordinarily refer to burdens related to high barriers to entry (such as capital requirements for financial and banking companies), or regulatory costs. In this Bill, however, the relaxing of data protection provisions for data fiduciaries would lead to restrictions of the privacy of individuals. Limitations to fundamental rights on grounds of 'fostering innovation' is not a constitutional tenable position, and contradict the primary objectives of a data protection law.

Chapter VIII- DATA PROTECTION AUTHORITY OF INDIA

- **Clause 42 (2): Composition and qualifications for appointment of members**

Comments: The composition of the members of the Selection Committee for the selection of members to the Authority has been drastically changed from the 2018 Bill leading to a potential significant reduction in the independence of the Authority. As per the 2018 Bill[42], the Selection Committee consisted of 3 members (i.e, the Chief Justice of India, the Cabinet Secretary and one expert of repute.) However, the present Bill has removed the judicial member and the expert from

[41] "A Data Sandbox for Your Company", Terrific Data, last accessed on January 31, 2019, http://terrificdata.com/2016/12/02/3221/

[42] Clause 50 (2) of the 2018 Bill states "*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.*"

the composition of the Selection Committee and it now comprises entirely of members from the Executive.

Recommendation: An independent Authority is the basis for a strong and robust data protection regime in the country, and it is therefore essential that the Selection Committee responsible for appointing the Authority is also perceived to be independent and neutral. We recommend that the composition of the Selection Committee be resorted to the composition under the 2018 Bill. Additionally, we **also reiterate our previous comments**: one eminent person representing the private sector and one eminent person representing the civil society are also made members of the committee.

- **Clause 43: Terms and Conditions of appointment**

Comments: The 2018 Bill[43] explicitly stated that the salaries, allowances and other terms and conditions of service of the chairperson and other members of the Authority would not be varied to their disadvantage during their term. This provision has been deleted from the current Bill.

For an efficient and smooth functioning of the Authority, it is necessary that the members of the Authority are able to function in an independent manner and are insulated from government control. By deleting the provision which prevented the government from varying the salaries and terms and conditions of appointment, the Central Government now has the power to reduce the salary or amend the terms of appointment to the detriment of the members of the Authority, thereby giving it effective control over the functioning of the Authority.

Recommendations: The 2018 provision should be reinstated and it should be clearly specified that the terms of appointments, salaries and allowances of the chairperson and members will not be varied to their disadvantage during the term of their appointment.

- **Clause 44: Removal of Chairperson or other Members**

Comments: The Central Government has been conferred the powers to remove from office the chairperson and or other members of the Authority on the basis of the grounds specified in the Bill. Considering that the Authority is required to exercise power over the Central Government as well as the State Government in exercise of their role as a data fiduciary, it is necessary to ensure that the power of removal does not solely vest with the Central Government.

[43] Clause 51 (2) of the 2018 Bill states "*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.*"

Recommendation: We **reiterate our earlier recommendation:** A committee similar to the one constituted for appointment of members must also be constituted to address any issues of removal of members.

- **Section 49: Powers and Functions of the Authority**

Comments: Unlike the 2018 Bill[44], under the present Bill, the power of the Authority to specify the residuary categories of sensitive personal data has been removed. This power has now been conferred upon the Central Government in consultation with the sectoral regulators and the Authority[45].

Further, the present Bill has reduced the powers and functions of the Authority from the powers specified under the 2018 Bill. Under the 2018 Bill, the functions of the Authority included (i) issuing guidance on provisions under the Bill either on its own or in response to a query from a data fiduciary; (ii) preparation and publication of reports setting out the result of any inspection or inquiry in public interest; and (iii) advising the Central Government on the acceptance of any relevant international instrument relating to protection of personal data. These functions of the Authority have been deleted from the present Bill. The rationale for deleting these functions is unclear.

Recommendations: We recommend that the provision as per the 2018 Bill should be reinstated and the Authority in consultation with the sectoral regulators should be empowered to determine further categories of personal data. Further, the deleted functions of the Authority should be reinstated and it should be required to publish the results of the inquiry which it deems to be in public interest. This is useful for[46] (a) data principals to identify how different data fiduciaries are approaching data protection; (b) the Authority to rectify if needed its rules and regulations; and (c) afford more trust and transparency to the Authority.

- **Clause 50: Codes of Practice**

[44] Clause 22 (1) of the 2018 Bill states "*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*".
[45] Clause 15(1) of the 2018 Bill states "*The Central Government shall, in consultation with the Authority and the sectoral regulator concerned, notify such categories of personal data as "sensitive personal data.*"
[46] Dvara Research, *supra*, page 10

Comments: Under the 2018 Bill[47], the Authority had the power to issue a code of practice regarding the mechanism for processing personal data of users who are incapable of providing valid consent. This power of the Authority has been removed from the present Bill. The rationale for the deletion of the power is unclear.

Recommendation: The power to issue a code of practice to develop an appropriate mechanism for processing of personal data of users who are incapable of providing valid consent should be reinstated. In addition, **we reiterate our previous comment:** The following categories of bodies be included in this provision as bodies who may submit codes of practices: academic and research organisation, particularly those working on issues of privacy, security and encryption; civil society bodies which are engaged in research or building awareness on privacy and data protection issues.

- **Clause 55: Search and Seizure**

Comments: Clause 55(4) provides that the Inquiry Officer can keep in its custody the seized material for a period not later than the conclusion of the inquiry. Under the 2018 Bill[48], the seized material could only be retained for six months (unless the Authority approved the retention for a longer period). Further, under the 2018 Bill[49], the person from whom the material had been seized could make copies of such material. This provision has been deleted under the present Bill.

Recommendations: A time period should be specified beyond which the seized materials cannot be kept in the custody of the Inquiry Officer. The provision in the 2018 Bill should be reinstated. In addition, the right of person to make copies of the seized material should also be reinstated into the present Bill.

- **Clause 62: Appointment of Adjudicating Officer**

[47]Clause 44 (6) of the 2018 Bill states "*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 (h) processing of personal data under any other ground for processing, including processing of personal data of children and development of age-verification mechanism under section 23 and mechanisms for processing personal data on the basis of consent of users incapable of providing valid consent under this Act.*"

[48] Clause 66(5) of the 2018 Bill states "*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.*"

[49] Clause 66(7) of the 2018 Bill states "*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 designated in this behalf.*"

Comments: Clause 62(2) provides that the Central Government shall be responsible for prescribing the number of adjudicating officers to be appointed, the manner and term of their appointment and the jurisdiction of such officers.

Recommendations: We reiterate our previous comment: Such powers should vest with the Authority instead of the Central Government.

Chapter XIII- OFFENCES

- **Clause 82: Re-identification and processing of de-identified personal data**

Comments: Clause 82(1) restricts the offences to re-identification and re-identification and processing of personal data. The offences relating to intentionally or recklessly obtaining, transferring or selling either personal or sensitive personal data has been deleted.

Recommendations: We reiterate our earlier recommendations: This clause could specify that whenever the personal data of a data principal was re-identified or de-identified the authority conducting such process must notify the data principal of such processing. Secondly we suggest the addition of another subsection to provide exemptions for research. We suggest the following language for the proposed subsection 3:"*Notwithstanding anything contained subsection (1) and (2) research undertaken for a re-identification and de-identification after notification of authority shall be exempt from the above provision. Provided that the researchers do not disclose or share any re-identified or de-identified data without consent of the data principals*."

- **Clause 83: Offences to be cognizable and non-bailable**

Comment: Clause 83(2) provides that no court shall take cognizance of any offence under this Bill, save on a complaint made by the Authority. The 2018 Bill[50] had no such provision; it merely provided that the offences shall be cognizable and non-bailable. The rationale for the inclusion of such a provision is unclear. Prior to the 2019 amendment to the Aadhar Act, the courts could take cognizance of a complaint, only if the Unique Identification Authority of India filed a complaint. The 2019 amendment changed this and has now permitted concerned individuals to file a complaint with the court directly. It is pertinent to note that this was pursuant to the 2018 Supreme Court judgement in Puttaswamy II,[51] in which the Supreme Court had held that it would be appropriate if the Aadhar Act was

[50] Clause 93 of the 2018 Bill states "*Notwithstanding anything contained in the Code of Criminal Procedure, 1973, an offence punishable under this Act shall be cognizable and non-bailable.*"
[51] Puttaswamy II, *supra*, page 427

amended and the concerned individual whose right is violated is permitted to file a complaint and initiate proceedings.

Recommendations: We recommend that this provision should be deleted. The power to file a complaint under the Bill should not be restricted to the Authority; the concerned person should also have the power to file a complaint directly without having to first approach the Authority.

- **Clause 85: Offences by State**

Comment: Clause 85 of the present Bill is different from the 2018 Bill such that it requires the offence to be "proved" in order to be held guilty under the Act. Under the 2018 Bill[52], the provision came into force when an offence was committed.

The new requirement to "prove the offence" is ambiguous and unclear.

ChapterXIV-Miscellaneous

- **Clause 86: Power of Central Government to issue directions**

Comment: Clause 86 gives the Central Government the power to issue directions to the Authority as necessary in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order. Though the Authority has the ability to express views on any direction, the decision of the Central Government - whether policy or not will be final and binding. In effect this provision severely undermines the strength and powers of the Authority. Given that the binding directions will pertain to security of the State etc. - the provision opens up the scope of exceptions defined in clause 35 and the already limited safeguards to the same - to potential revision. This could have serious implications for human rights.

Recommendation: We recommend that this provision is deleted.

- **Clause 92: Bar on processing certain forms of biometric data**

Comments: The clause prohibits data fiduciaries from processing such biometric as may be notified by the Central Government, unless such processing is permitted by

[52] Clause 96 (1) of the 2018 Bill states "*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.*"

law. It is unclear as to why such a bar has only been placed on processing of biometric data and not on processing of other forms of genetic and sensitive personal data.

Recommendation: We recommend that this provision be revised to lay out the circumstances under which the Central government may place a bar on any form of sensitive personal data and also specify the principles to guide the same.

Clause 93: Central Government Power to make rules

Recommendation: This clause defines 25 instances in which the Central Government has the power to make rules to carry out the provisions of the Bili. Of these, we would recommend the deletion of:

- the methods of voluntary identification to identify users of social media under sub-clause (3) and the identifying mark of verification of a voluntarily verified user under sub-clause (4) of clause 28;
- the entity or class of entity in a country, or international organisations to which transfers may be permitted under clause (b) of sub-clause(1) of clause 34;

We suggest shifting the following to the Authority:

- any other categories of sensitive personal data under clause 15;
- other factors to be taken into consideration under clause (d) of sub-clause(3) of clause 16.