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

The Personal Data Protection Bill

28 July, 2018

By **Amber Sinha, Elonnai Hickok, Shweta Mohandas, Arindrajit Basu**

Inputs from **Pranesh Prakash**

Edited by **Pranav M. Bidare**

Research Assistance by **Shreeja Sen**

The Centre for Internet and Society, India

Introduction

The Centre for Internet and Society is a non-profit research organisation that works on policy issues relating to privacy, freedom of expression, accessibility for persons with diverse abilities, access to knowledge, intellectual property rights and openness. It engages in academic research to explore and affect the shape and form of the Internet, along with its relationship with the Society, with particular emphasis on South-South dialogues and exchange.

CIS has conducted extensive research into the areas privacy, data protection, data security, and was also a member of the Committee of Experts constituted under Justice A P Shah. CIS has also been cited multiple times in the Report of the Committee of Experts led by Justice Srikrishna. CIS values the fundamental principles of justice, equality, freedom and economic development. This submission is consistent with CIS' commitment to these values, the safeguarding of general public interest and the protection of individuals' right to privacy and data protection. Accordingly, the comments in this submission aim to further these principles. We welcome the opportunity provided to our comments on the Bill and we hope that the final Bill will consider the interests of all the stakeholders to ensure a Bill that protects the privacy of the individual while encouraging a free and fair economy.

Section Wise Comments and Recommendations

The Personal Data Protection Bill provides for the establishment of a Data Protection Authority to oversee activities that involve processing of data. It also recognises the need to protect personal data under the fundamental right to privacy, as well as the need to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress and innovation. Additionally, the Bill states that it aims to protect the autonomy of individuals in relation with their personal data, to specify where the flow and usage of personal data is appropriate, to create a relationship of trust between persons and entities processing their personal data, to specify the rights of individuals whose personal data are processed, to create a framework for implementing organisational and technical measures in processing personal data, to lay down norms for cross-border transfer of personal data, to ensure the accountability of entities processing personal data, and to provide remedies for unauthorised and harmful processing.

CHAPTER I PRELIMINARY

Section 3: Definitions

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

- **Section 3 (19): Financial Data**
  Comments: Section 3 (19) of the Bill defines financial data as *any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal or any personal data regarding the relationship between a financial institution and a data principal including financial status and credit history*. 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 recommend that 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.

- **Section 3 (29): Personal Data**
  Comments: Section 2 (29) of the Bill defines personal data as "*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 persona 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.[1]
"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 recommend that 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.[2] We recommend the below 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."

- **Section 3 (3): Anonymisation**
  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, meeting the standards specified by the Authority."*

[1] "What is personal data?" European Commission <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en>
[2] "What is personal data?" European Commission <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en>

Comments: The definition of anonymisation needs to protect privacy while enabling to scientific research and innovation .
Recommendations: 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 re-identify individuals,[3] as has been called out by many experts including the Sri Krishna Committee.[4] 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."[5] 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 concerns community privacy concerns and thus fair and reasonable processing obligations would still need to apply.

- **Section 3 (9): Child**
The Bill defines a child as "a data principal who is below 18 years of age."
Comments: This definition does not account for the realities of how children interact with the digital.The age where a child can give consent to data processing must not be equated with maturity as defined in the Indian Contract Act.[6] Children interact with data fiduciaries from a much younger age than 18 and requesting age verification and parental consent can undermine a child's ability to understand and choose how their data is being used.[7] The GDPR under Article 8 states that in the processing of the

[3] Arvind Narayanan and Vitaly Shmatikov, "Robust De-anonymization of Large Sparse Datasets" <https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf>; Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006>.
[4] A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians., Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, 28, <http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf>
[5] Art. 5 III, Proteção de Dados pessoais, 2018 <https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf>
[6] Section 11, Indian Contract Act, 1872.
[7]https://www.hindustantimes.com/analysis/india-needs-to-acknowledge-the-gaps-in-data-protection-and-rights-of-children/story-bxBrYtqXylgPou2yADe3xJ.html

personal data of a child shall be lawful where the child is at least 16 years old, where the consent is given or authorised by the holder of parental responsibility over the child. The GDPR also allows member states to lower the age to 13 years.[8] The other problematic provision is of considering all data principals under the age of 18 to be minors.[9] The 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 justifies it by stating that the relationship between a person and the state cannot be reduced to a contract.[10] 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: 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 to 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.

- Terms that the Bill does not define or leaves for further defining by the Authority or Central Government include:
    - 'Data trust score' as under sections 8(1)(m), 30(1)(f), 35(5), 35(6), 60(2)(f), 60(2)(g), 108(2)(u).
    - 'Critical data' as under section 40(2).

[8] Art. 8, General Data Protection Regulation, 2018.
[9] A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians., Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, 44, <http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf>.
[10] "The interaction between the state and the citizen in this context cannot be compared to that of a consumer entering into a contract with a service provider.", A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians., Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, 108, <http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf>.

Chapter II - Data Protection Obligations

- **Section 4: Fair and reasonable processing**
  This section holds that 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.
  Comments: This is among the most important provisions in the Bill as it has application across provisions. Even in cases where certain kinds of processing of data are exempt from data protection obligations of the fiduciaries and processors, Section 4 continues to apply. Provisions such as those that allow non consensual processing of data such as Section 13(Processing of personal data for functions of the State), Section 16(Processing of personal data necessary for purposes related to employment) ect. do not negate the responsibility of the data fiduciary to ensure fair and reasonable processing. Therefore, it is important that this provision reflects the standard of 'harm' that has been incorporated throughout the Bill including in the Introduction, Further categories of sensitive personal data, the principle of Privacy by design, the principle of Transparency etc.
  Recommendations: We recommend 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. Suggested 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.*

- **Section 5: Purpose limitation**
  Comments: Section 5 (1) states that personal data shall be processed only for purposes which are clear, specific and lawful. As purpose limitation and informed consent are central to the conceptual structure of this bill, it is necessary that the bill provides further guidance on how these terms may be interpreted. Section 5(2) of the Bill states that the personal data shall be processed only for purposes specified or for any other incidental purpose that the data principal would reasonably expect the personal data to be used for, having regard to the specified purposes, and the context and circumstances in which the personal data was collected . The incidental purpose is a very wide standard and it needs to be narrowed down.

Recommendations: We recommend that the Bill provides guidance on the standards of 'clear', 'specific' and 'lawful' and that further the Data Protection Authority has a responsibility to publish and provide guidance on the standards of 'clear', 'specific', and 'lawful' as clearer definitions evolve through use cases the Authority evaluates in its 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. 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 harms to the data subjects

- **Section 6**: **Collection limitation**
  Comments: Section 6 states that the collection of personal data shall be limited to such data that is necessary for the purposes of processing. The provision currently does not incorporate the standard of 'proportionate' - thus potentially allowing for overcollection tied to overly broad purposes.
  Recommendations: We would recommend that the test of proportionality be also added under this Section 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.*

- **Section 8**: **Notice**
  This section specifies how notice shall be provided to the data principal and what should be contained in the notice.
  Comments: In addition to the comprehensive categories listed in the Bill, there is other information that, if provided, would further enable the individual to take informed decisions regarding their data and associated rights. This includes information about whether the provisions are contractual, the existence of automated decision making.
  Recommendations: 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. Section 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 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.[11] 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.[12] 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.

Chapter III GROUNDS FOR PROCESSING OF PERSONAL DATA

- **Section 12: Processing of personal data on the basis of consent**
  Comments: This section 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

[11] General Data Protection Regulation, 2018.
[12] A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians., Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, 75, <http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf>.

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. Section 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 sections does 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.[13] 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.[14]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: Section 12 could state that the consent needs 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[15] 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. As suggested by Daniel Solove[16] the data principal can be notified of the types of new uses of the data she provides, and this guidance can be provided by law. Instead of a blanket

---

[13] A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians., Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, 38-40, <http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf>.

[14] Ibid.

[15] A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians., Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, <http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf>.

[16] Solove, D. J. (2012). Introduction: Privacy self-management and the consent dilemma. Harv. L. Rev., 126, 1880. <https://pdfs.semanticscholar.org/809c/bef85855e4c5333af40740fe532ac4b496d2.pdf>

consent a graded approach could be taken where processing can be qualified as those that must not be done, those that require consent a new, those where the data principal has a right to revoke consent and those that can be permitted without consent.[17]

- **Section 13: Processing of personal data for the functions of the state**
  Comments: Section 13(1) of the Bill states that personal data may be processed if such processing is necessary for any function of Parliament or any State Legislature. Section 13(2) of the Bill states that personal data may be processed if such processing is necessary for the exercise of any function of the State authorised by law for providing service or benefit to the data principal or for the issuance of any certification, license or permit for any action or activity of the data principal by the State.
  Recommendations: Under subsection 2, the conditions for the non consensual processing should not just rely 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. The report of the DP Bill states that the processing of data by the state must be strictly that which is necessary and is proportionate to the legitimate purpose at hand.[18] Hence we suggest that this test of necessity and proportionality for the non consensual processing of data be reflected not only in the report of the Bill but also in the provision of the Bill.
  We suggest that the provision of the Bill be worded as follows:
  Suggested language: *Personal data may be processed if such processing is necessary and proportionate—*

- **Section 14: Processing of personal data in compliance with law or any order of any court or tribunal.**
  Comments: This section states that personal data may be processed if such processing is explicitly mandated under any law made by Parliament or any State Legislature; or (b) for compliance with any order or judgment of any Court or Tribunal in India. This section should state that the processing is not just conditional upon necessity but also proportionality.

---

[17] Solove, D. J. (2012). Introduction: Privacy self-management and the consent dilemma. Harv. L. Rev., 126, 1880. <https://pdfs.semanticscholar.org/809c/bef85855e4c5333af40740fe532ac4b496d2.pdf>

[18] A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians., Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, 111 <http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf>.

- **Section 15: Processing of personal data necessary for prompt action**
  Recommendations: We recommend that the legal standard of necessity is buttressed with the standard of proportionality such that the first line of the provision reads as follows:
  Personal data may be processed if such processing is necessary and proportionate—

CHAPTER IV GROUNDS FOR PROCESSING OF SENSITIVE PERSONAL DATA

- **Section 19: Processing of sensitive personal data for certain functions of the State**
  Comments: This section states that sensitive personal data may be processed if such processing is strictly necessary for any function of Parliament or any State Legislature or for the exercise of any function of the State authorised by law for the provision of any service or benefit to the data principal. However 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.
  Recommendations:
    - It is imperative that test of proportionality is also included along with the test of necessity.
    - The use of the term “strictly necessary” in Chapter IV needs to be clarified. It is not clear how this standard is different from that of ‘necessary’ which is used in Chapter III.

- **Section 20: Processing of sensitive personal data in compliance with law or any order of any court or tribunal**
  Comments: This section states that the sensitive personal data may be processed when such processing in necessary for compliance with any order or judgment of any Court or Tribunal in India. However the test of necessity should not be the only test with the processing of sensitive personal data.
  Recommendations: It is imperative that test of proportionality is also included along with the test of necessity and proportionality. The use of the term “strictly necessary” in Chapter IV needs to be clarified. It is not clear how this standard is different from that of ‘necessary’ which is used in Chapter III.

- **General Recommendations**: As stated in our recommendation for Section 13, in Sections 16, 17, 18, 19, 20, 21 the grounds for processing should include

both necessity and proportionality. Both the necessity and proportionality needs to be the two conditions that are imperative for non consensual data protection. We suggest that all the provisions that deals with non consensual processing in the Bill should contain the following line: Suggested language: *Personal data may be processed if such processing is necessary and proportionate—*

CHAPTER V PERSONAL AND SENSITIVE PERSONAL DATA OF CHILDREN

- **Section 23: Processing of personal data and sensitive personal data of children**
  Comments: This section states that appropriate mechanisms and age verification and parental consent with respect to the data of children under 18 years of age.However the Bill does not make provisions for the data principal to withdraw the consent that was given by her parents on her behalf.
  Recommendations: We suggest that the data principal on attaining majority(according to the Act) have 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.[19]

CHAPTER VI DATA PRINCIPAL RIGHTS

- **Section 24: Right to confirmation and access**
  Comments: Subsection 1 of the Bill states that the data principal has the right to access from the data fiduciary a brief summary of the personal data of the data principal that is being processed as well as the processing activities undertaken by the data fiduciary 24(1)(a) and (b). 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.

[19] Section 8(2), Indian Privacy Code, 2018 <https://saveourprivacy.in/bill>

Recommendations: It is recommended that the phrase 'a brief summary of' in Section 24 (b) is replaced with 'a copy of' such that it reads: *a copy of the personal data of the data principal being processed or that has been processed by the data fiduciary*. Further, we recommend the addition of sub clause (c) which states as follows: *an explanation of the how the processing is justified under one or more of the provisions under Chapters III and IV*.

- **Section 27: Right to Be Forgotten**
  Comments: Section 27 of the Bill states that the data principal has the right to restrict or prevent continuing disclosure of personal data by a data fiduciary related to the data principal...". However 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 suggest the following recommendations to the Section 27:
    1. This Section'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 could provide the data principal with the right to be forgotten, by obtaining from the data fiduciary the deletion of the personal data concerning her without undue delay. The Data Protection 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:** Additionally we also recommend the inclusion of the following rights in Chapter V.

    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 Section 13, Section 17 and Section 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 VII TRANSPARENCY AND ACCOUNTABILITY MEASURES

- **Section 29: Privacy by Design**
Comments: This section states the policies and measures that every data fiduciary shall implement to create and implement a framework of privacy design within the organization . However this Bill should not only ensure that the data fiduciary prioritises privacy by design but also privacy by default.
Recommendations: The provisions under this section state the various policies and measures that data principals need to implement. We suggest that the Bill not only emphasise on privacy by design but also 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.[20]

[20] Article 25(2), General Data Protection Regulation, 2018.

2. The data fiduciary especially those that process sensitive personal data must practice data minimisation, and implement measures such as anonymisation.[21]

- **Section 32: Personal Data Breach.**
  This section provides that the data fiduciary must compulsorily notify the DPA once the occurrence of a breach has been detected.
  Comments:
  (1) The data fiduciary is not under an obligation to disclose all personal data breaches-only those likely to cause "harm to any data principal." The term 'harm' has not been defined in this sub-section and the difference in threshold between 'harm' and 'significant harm' defined in Section 2(37) remains unclear. Further, it provides the fiduciary with the discretion to decide whether a breach causes harm to a data principal or not. This discretion is also problematic from an insurance industry perspective. Cyber insurance could be a key tool in alleviating the stress caused to the financial sector through cyber vulnerabilities across the supply chain. However, the industry would suffer from a lack of data if breaches are not reported, which would prevent an adequate rating of insurance.[22]
  (2) Unlike the GDPR, which imposes a 72 hour time limit on notifying a data breach to the supervising authority[23], the SriKrishna Bill has no such requirement. This is a positive departure as it has been widely argued that 72 hours is too short a time period to detect a data breach, identify its scope and impact and make a representation to the supervising authority detailing remedying steps being undertaken by the entity that has been breached.[24] However, the provision 32(3) states that 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 Section 60.
  (3) Section 32(5) states that the DPA may choose to compel the fiduciary to report the breach to the data depending on the severity of the breach, the harm likely to be caused to the data principal and any

[21] Ibid.
[22] Caitriona Heinl, " Key observations to enhance cyber resilience" (March 2018,NTU Cyber Risk Management Report),http://irfrc.ntu.edu.sg/Research/cyrim/Pages/Home.aspx
[23] Art 33(1), General Data Protection Regulation, 2018.
[24] S. Ryan, "72 Hours: Understanding the GDPR Data Breach Reporting Timeline", 2018 <https://www.imperva.com/blog/2018/05/72-hours-understanding-the-gdpr-data-breach-reporting-timeline/>

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 DPA 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 DPA may be ill-equipped to determine. Second, again 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: (1) In Section, 32 (1), delete **"**where such breach is likely to cause harm to any data principal.
(2) Impose a reasonable time limit on the data fiduciary to report data breaches under Section 32(3) or empower the DPA to decide time limits under Section 60.
(3) Instead of enabling the DPA to decide when to notify the breach to the data principal, amend 32 (5) to make this disclosure mandatory. The DPA should be allowed to withhold this information only in the case of narrowly defined exceptions such as national security.

- **Section 39**: **Grievance Redressal**
  Comment: This section 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.
  Recommendation: We suggest the inclusion of a list of key mechanisms to be added to this section including::
  Suggested 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 VIII: Transfer of Personal Data Outside India

- **Section 40: Restrictions on Cross-Border Transfer of Personal Data**
  Comments: This section adopts a three-pronged model delineating the transfer of data outside India. First, as per Section 40(1) all personal data to which the Bill applies must have at least one live, serving copy stored inside India. Second,with regard to certain categories of personal data to be notified as 'critical personal data' by the central government under Section 40(2), there is a mandate to store and process this personal data only in

India such that no transfer abroad is permitted. Third, under Section 40(3) the Central government has been bestowed with the power to exempt transfers on the basis of strategic or practical concerns, thereby enabling the free flow of data when they deem it to be justified.

Comments: This submission is not meant to serve as a blanket criticism of data localisation, in circumstances which benefits India's strategic interests and is clearly defined in a sector-specific law or regulation in which case the costs and benefits of having a localisation provision can be evaluated keeping the context in mind. However, the 'one-size-fits-all' approach to data localisation with the vesting of carte blanche' authority on the government to determine exemptions and export prohibitions is unjustified. In particular, allowing these questions to be delegated to agencies of the Central Government rather than voted on and passed by the Legislature opens the government up to allegations of excessive delegation to the Executive of legislative responsibility and consequently, a lack of effective representation in the passage of crucial provisions of a law with wide-ranging ramifications.[25]A more restrained approach to localisation is required, which should be determined by sectoral regulators after consultation with crucial stakeholders that may be impacted by localisation requirements.

1. The SriKrishna Committee Report offers five justifications for imposing mandatory localised requirements.[26] We submit that each of these objectives set out are either misplaced or attainable through less onerous means.

   A pointed rebuttal to each of the justifications offered follows:

   a. *Enforcement*

      Access to data by domestic law enforcement authorities is a laudable goal. As recognised by the White Paper, a disproportionate amount of data belonging to Indian citizens is stored in the United States and the presently existing Mutual Legal Assistance Treaties process (MLATs) through which Indian law enforcement authorities presently gain access to data stored in the US is excessively slow and cumbersome. However, it is unlikely that the localisation mandate will solve this issue for two reasons. First, as recognised by the Committee itself, a conflict of law question

[25] Greenleaf G, GDPR-Lite and GDPR-Lite and Requiring Strengthening – Submission on the Draft *Personal Data Protection Bill* to the Ministry of Electronics and Information Technology (India) Retreived from *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3252286n*

[26] A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians., Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, 88-96, <http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf>

may still arise despite the data being physically stored in India. First, the country where the mirror copy is stored will retain its right to assert territorial jurisdiction. Further, given the lack of a clear hierarchy between the other permissive principles of extra-territorial jurisdiction[27], which means that the country where the company is located in might assert jurisdiction, despite the data being stored physically in India. Technology companies located in the US will still be able to provide access to the data once they obtain a warrant from federal authorities. The Report seems to assert that the odds of a foreign entity refusing access to the data will be reduced if this provision is enforced as India will have a stronger claim in International Law and also help make a case for any conflict to be resolved by an Indian court. While this assertion may be theoretically correct,there is no evidence to suggest that a stronger position in International Law will necessarily foster better compliance. Instead, India would fare better if it were to use the language of international law to articulate its position better in diplomatic negotiations to reform the MLAT process[28] or propel itself to a better position in the CLOUD Act rather than damage goodwill by implementing this onerous measure.[29]

Second, the localisation mandate only extends to relating to Indian citizens. It does not solve the problem, that arose in the *Microsoft-Ireland* case[30] where law enforcement agencies required access to data relating to a foreigner. Therefore, given the onerous costs of the requirement and the possibility of resolving it more efficaciously through diplomatic channels, it is not clear if the Committee's reasoning is enough to justify localisation in this case.

b. *Avoiding vulnerabilities of relying on fibre optic cable network*

The report cites studies which suggest that undersea cable networks that transmit data from one country to another are

---

[27] M. Kamminga, 'Extraterritoriality', in Wolfrum, R. (ed.), Max Planck Encyclopaedia of Public International Law, (Oxford University Press, Oxford, 2010).

[28] A. Sinha, and ors., Cross Border Data-Sharing and India, Centre for Internet and Society, 2018 <https://cis-india.org/internet-governance/files/mlat-report>

[29] E. Hickok, and V. Kharbanda, An Analysis of the CLOUD Act and Implications for India, Centre for Internet and Society, 2018 <https://cis-india.org/internet-governance/blog/an-analysis-of-the-cloud-act-and-implications-for-india>

[30] A. Basu, The Microsoft-Ireland Ruling is a game changer for data protection and #MLAT regimes, July 18 2016 <https://www.orfonline.org/expert-speak/the-microsoft-ireland-ruling-is-a-game-changer-for-data-protection-and-mlat-regimes/>

vulnerable to attack. Therefore, processing critical data on Indian territory would minimise the vulnerability of relying on undersea cables. It cites a report by Policy Exchange that states that the threat-to undersea cables by Russian actors may be an existential one for the UK.[31] However, it does not engage with the solutions offered by the same report, which largely suggest improving the UK's defense and security posture and co-operating with global partners and allies to protect these underwater cables.The recommendations offered by the report for developing United Kingdom's strategy in this domain include :

i. Undertake a large scale strategic review that maps risks to this infrastructure and identify steps that UK has taken to mitigate these risks
ii. Update the National Risk Assessment and Risk Register
iii. Secure landing sites
iv. Establish Cable Protection Zones (CPZ) in collaboration with international partners in areas with high value communication corridors, not only around the UK but also in strategic geo-strategic nodes such as the Mediterranean and the Suez
v. Improve the quality of equipment deployed on cables
vi. Work with the private sector to increase the geographic diversity of undersea cables by increasing the number of landing sites, thus averting over-reliance on a few choke points
vii. Encouraging the private sector to build back-up cables
viii. Working to improve the piecemeal International Law regime securing undersea cables.

These suggestions, rooted in international diplomacy and security measures are valuable lessons for India as well. India cannot simply 'localise away' the challenges posed by the vulnerabilities in sea-cables.[32] Further, without a comparative assessment of the threat vectors and resilience of the Indian data processing facilities and that of underwater sea cables, this cannot serve as a justification for data localisation. Instead, as pointed out by the Report itself, the security of underwater sea cables is increasingly being recognised as a

[31] R. Sunak MP, Undersea Cables, Policy Exchange, 2017, 5 <https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf>
[32] G. Hinck, Evaluating the Russian Threat to Undersea Cables, March 5, 2018 <https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables>

global issue, which indicates that other countries and the private sector will all retain an interest in ensuring security of these cables, whereas India will be solely responsible for data servers stored within its territory.

c. *Building an AI ecosystem*
The Report makes the point that storing and processing data will enable India's AI ecosystem, that is at present largely composed of private sector actors, to harness this data. It remains unclear, however, whether merely storing a copy of data on Indian servers will guarantee availability of this data to the ecosystem.Further, there may be a significant economic cost to start-ups if other countries were to impose similar laws as they would not be able to harness data being stored or processed in other jurisdictions. Indeed, this data localisation provision may impact the outcome of ongoing trade negotiations such as the Regional Comprehensive Economic Partnership (RCEP) and would prevent India's AI ecosystem from benefitting from the free flow of data across RCEP countries if this provision were to become law.

d. *Preventing foreign surveillance*
The Report argues that storing personal data within and restricting the storing and processing of data within Indian territory may protect foreign surveillance from agencies largely headquartered in the US. This position reflects a misunderstanding of how foreign surveillance works and may end up offering more opportunities for this practice. First, compelled localisation may reduce the quality of security provided by local service providers.[33] Global companies will have to opt for local service providers who are shielded from global competition by the localisation requirements and may therefore have weaker security measures in place, thereby making them an easier target for foreign surveillance agencies. Further,having localized data servers reduces the opportunity to distribute information across multiple locations, Information gathered in one location offers a Honeypot opportunity for both criminals and foreign intelligence agencies alike.

Recommendations: Instead of opting for a 'one size fits all' data localisation provision, further interdisciplinary research is needed to map the complex symbiosis between international factors and domestic requirements that

[33] A Chander and U.Le, " Breaking the Web: Data Localisation v the Global internet" Retreived from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858.

might enable India to develop a sector and context-specific approach to data localisation.

Chapter IX: Exemptions

- **General Comments**: Chapter IX of the Bill provides for exemptions to various provisions of the Bill in cases of processing of data required for the Security of the state, Prevention, detection, investigation and prosecution of contraventions of law, Processing for the purpose of legal proceedings, Research, archiving or statistical purposes, Manual processing by small entities and Personal or domestic purposes. We welcome the Committee's suggestions to include the twin tests of 'necessity' and 'proportionality' as condition precedent for any processing for the purposes of the Security of the state; and Prevention, detection, investigation and prosecution of contraventions of law. However, we would strongly recommend that the following substantive provisions are included with the scope of Section 42 and 43:
    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 for 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 be required to examine all requests for processing under Section 42 and 43, and be subject 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 Section 42 and 43.
    d) Exemption under Section 42 and 43 need not be as sweeping as they have been drafted currently. We recommend that there is no need to exempt all accountability measures under Chapter VII. Requirements such as reporting personal data breaches to the Authority and data audits should continue to apply.
    e) Further, we recommend that exemption from Chapter VIII on cross border transfers should not be applicable in the case of Section 42

and 43, as they have the potential to dilute international safeguards for cross border flow of data.

f) We also recommend that user notifications rights be made available under both Sections 42 and 43. Such notification may be 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 Sections 42 and 43.

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

- **Section 59**: Furnishing of returns, etc. to Central Government
  Comments: Section 59(2) and of the Bill states that the DPA shall prepare an annual report giving a summary of its activities and copies of the report shall be forwarded to the Central Government and before each House of the Parliament. However the Bill does not mandate the annual reports to be made public.
  Recommendations: To ensure transparency in the functioning of the DPA we suggest that the annual reports be made public.Such disclosure is crucial to ensure that the public is able to make informed decisions. Categories that could be included in such reports include: number of data fiduciaries, number of data fiduciaries that have carried out Impact Assessment, the fines collected as penalties, data fiduciaries that have been fined, fiduciaries transferring data abroad the number of data breaches to name a few.

Chapter X: Data Protection Authority of India

General Comments:

A. Responsive Regulation

While the Report endorses regulatory framework equipped with a range of tools, as recommended by us in our Response to the White Paper, we were disappointed to see only minimal application of this framework in the Bill. We concur with Prof. Graham Greenleaf's analysis,[34] which has fleshed out how the 'responsive regulation' approach can be used in data protection frameworks and he speaks to three kinds of measures needed:

[34] Graham Greenleaf, Responsive Regulation of Data Privacy: Theory and Asian Examples. In David Wright, Paul de Hert, (Ed.) (2016) Enforcing Privacy: Regulatory, Legal and Technological Approaches. Springer.

- Reactive measures that respond to breaches or legal requirements,
- Systemic or proactive measures that take steps aimed at detecting and preventing breaches, and
- Positive or supportive measures like training, awards etc. to support those trying to comply with regulatory goals.

While the Bill speaks about reactive measures in great detail, there is relatively little by way of systemic and supportive measures. In the 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 kind of inexpensive and innovative strategies. We recommend the following additional powers for the Authority to be clearly spelt out in the Bill:

Informal Guidance

It would be useful for the Authority to set up a mechanism on the lines of Securities 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 the first omnibus data protection law in India, and there is very little jurisprudence on the subject in India, it would be extremely useful for regulated entities to get guidance from the regulator.[35]

Power to issue Notices and Warnings

A regulator may require an organisation to provide it with whatever information it needs to carry out its functions. This is sometimes described as an "information notice". It differs from an "enforcement notice", whereby the regulator may require a data controller or data processor to take whatever steps it considers appropriate to comply with data protection legislation. Such steps could include correcting data, blocking data from use for certain purposes, or erasing data altogether. In Ireland, the Office of the Data Protection Commissioner (ODPC) may prohibit the transfer of personal data from the state to a place outside the European Economic Area.

[35] M. Raghavan, (2018) Data Protection: Before The Horse Bolts, Bloomberg Quint. <https://www.bloombergquint.com/opinion/data-protection-before-the-horse-bolts#gs.UeJHS48>.

The ODPC can exercise this power by providing a written notice, called a "prohibition notice", to the data controller or data processor. In considering whether to exercise this power, the ODPC considers the need to facilitate international transfers of information. A prohibition notice may be absolute, or may prohibit the transfer of personal data until the person concerned takes certain steps to protect the interests of the individuals affected.

An enforcement notice has the potential to have a far greater influence on a controller than even the heftiest fine: an order to cease processing personal data altogether. Whether the order only relates to certain types of data, or is confined to a limited period (for example, until the controller improves its compliance more generally), it has the potential to shut down a business for the duration of the notice. Consequently, this power is often regarded as the strongest weapon that a DPA has in its arsenal. Failure to comply with an enforcement notice is punishable by a fine, and constitutes a criminal offence. This means that any subsequent fine is potentially unlimited, but would have to be the subject of formal proceedings before a criminal court (entailing, amongst other things, that the offence be proved beyond reasonable doubt).

Power to name and shame

When a DPA makes public the names of organisations that have seriously contravene 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 website for journalists to find, but frequently issues press releases, briefs journalists and uses social media. The ICO's public policy statement on communicating enforcement activities states that "the ICO aims to get media coverage for enforcement activities".

Undertakings

The ICO has leveraged the threat of fines into an alternative enforcement mechanism seeking contractual undertakings from data controllers to take certain remedial steps. Although the practice began before fines were initially introduced, the regulator can encourage data controllers to take steps to avoid a fine and the resulting negative media coverage. 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 challenge 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.

B. Devolved Jurisdiction

The way the Authority is structured in its current formulation in the bill leads to a position where there a small regulator of seven members is responsible for performing functions and discharging powers that range from receiving complaints and investigations to issuance of codes of practices and guidance to technical trainings and awareness. While the Authority has powers to appoint officers, employees, consultants and experts as required, the current systems of regulation is too centralised. We propose the following steps to create a more devolved and decentralised systems of regulation:

a. Creation of State Data Protection Authorities

The Data Protection Authority has wide powers and jurisdiction and will have to blend the features of a public facing regulator which receives complaints and discharges justice such as the Central and State Commissions under the Rights to Information, Act, and the Consumer Disputes Redressal Commision under the Consumer Protection Act. On the other hand, like regulator such as Securities and Exchange Board of India, the Authority is also required to provide guidance, issues notices and monitor the data ecosystem closely. Therefore a single centralised body may not be the appropriate form of such a regulator. We propose that the 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 of respond to local complaints and exercise jurisdiction over entities within their territorial jurisdictions.

b. 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, an association representing the interest of data principals, any sectoral regulator or statutory authority, or any departments or ministries of the Central or State Government in the formulation of codes of practices. However, it would be useful to also have more active participation of industry associations and civil society bodies in activities such as promoting awareness among data fiduciaries of their obligations and duties under this Act, promoting

measures and undertaking research for innovation in the field of protection of personal data, specifying the criteria for assigning a rating in the form of a data trust score by a data auditor and formulation of anonymisation and de-identification standards.

C. Independence of the Authority

The Personal Data Protection Bill makes significant strides towards ensuring the creation of independence regulator, such as establishment of the Authority through a legislation, fixed term of office for members, defined process for removal of members, reporting requirements directly to the legislature, prohibition of on conflicts of interests, Subjecting the Authority's decisions to right to appeal. However, there are still provisions that need to be added or amended in order to ensure an independent regulator. We recommend the following measures:

a) Removal of members:
   Under Section 52, the power to remove members of the Authority vests with the Central Government. As the Authority is also required to exercise jurisdiction over government bodies including the central government, it is necessary to ensure that powers to remove members are not vested with the Central Government. We recommend that a committee similar to the one constituted for appointment of members must also be constituted to address any issues of removal of members,
b) More representative Selection Committee:
   Currently, the selection committee under Section 50 is not representative enough, and we propose that one eminent person representing the private sector, and one eminent person representing the civil society are also made members of the committee.
c) Composition of the Authority
   The Bill currently states that the members of the Authority shall be persons of ability, integrity and standing, and must have specialised knowledge of, and not less than ten years professional experience in the field of data protection, information technology, data management, data science, data security, cyber and internet laws, and related subjects. It is however, necessary that the Bill specifies that one member of the Authority shall have technological expertise in areas such as encryption, de-identification and data security.
d) Appointment of Adjudicating Officer
   Currently, the Bill provides for the Central Government to prescribe the number, qualification, manner of appointment, jurisdiction and

procedure of Adjudicating officers. However, we strongly recommend that these powers vest with the Authority instead.

- **Section 61**: Codes of Practice
  Comments: Subsection(2) of the Bill states that the Authority may also approve and issue codes of practice submitted by an industry or trade association, an association representing the interest of data principals, any sectoral regulator or statutory authority, or any departments or ministries of the Central or State Government.
  Recommendations: We also recommend that the following categories of bodies be included in this provisions 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.

CHAPTER XIII OFFENCES

- **General Comments**: Sections 90 - 96 to lays down the punishment for offences under the Bill. However these Sections enforce punishments without providing a cooling down period for data fiduciaries to comply with the provisions of the Act. 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 Data Protection 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 DPA 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.

- **Section 92: Re-identification and processing of de-identified personal data**
  Comments: Subsection 2 of this section states about the exemptions to such re-identification and de-identification. However this section does not make provisions for the data principal to be notified of such processing of

her personal data. Additionally this provisions does not provide exemptions for research purposes.

Recommendations: Subsection 2 of this section 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 would like to propose the addition of another subsection to provide exemptions for research. The proposed subsection 3 could read as follows:

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.