Responses dated 31 January 2018 to the "White Paper of the Committee of Experts on a Data Protection Framework for India" dated 27 November 2017 (White Paper) released by the Ministry of Electronics and Information Technology (MeitY)

Dvara Research[1] is an Indian not-for-profit policy research and advocacy institution guided by our mission of ensuring that every individual and every enterprise has complete access to financial services. Our work addresses emerging issues in policy and regulation for consumer protection, affecting individuals accessing finance in light of the sweeping changes that are reshaping retail financial services in India. The regulation and protection of consumer data in providing financial services has been a core area of our recent research.

In this document, we present our responses to the public consultation on the White Paper which is based on our broader approach on data protection. This approach looks past a consent-led approach to data protection, and seeks to embed a bundle of rights for all individuals with respect to their personally identifiable data that apply even where consent has been validly obtained for data collection. We also propose a contextual "legitimate purpose" test for India that must be applied by all entities who will have new obligations under such a regime, to allow the proper exercise of individuals' data rights. In addition we propose a model for supervision and enforcement that uses the full range of regulatory tools, before and after a data breach.

The nine points below set out the highlights of our mental model for a future data protection framework for India. Our responses to the questions posed in the White Paper reflect these points and expand upon them.

1. **Scope**: We propose that the law should apply to private and public entities. Foreign entities should be caught by the law in circumstances where (i) they conduct business in India, (ii) process personal data from India or (iii) process data for an Indian controller outside India. We also propose that the law should afford protections to all natural persons (citizens and residents) present in India.

2. **A single standard for personal data protection**: We propose that all personally identifiable data should be protected at the same level by the future data protection law. Personally identifiable information should not be categorised into "sensitive personal" data and "personal data" (as currently contemplated by the White Paper) which results in each category getting different levels of protection. This is important given that the sensitivity of data is heavily contextual and modern data

[1] Dvara Research (formerly the IFMR Finance Foundation) has made several contributions to the Indian financial system and participated in engagements with all key financial sector regulators and the Government of India. We were the technical secretariat to the RBI's Committee on Comprehensive Financial Services for Small Businesses and Low Income Households (**CCFS**) Chaired by Dr. Nachiket Mor. We also acted as peer reviewers for the customer protection recommendations made by the Financial Sector Legislative Reforms Committee (FSLRC).

Our team have benefitted from the intellectual engagement of several experts in the course of our research. We would like to thank Dr Katharine Kemp, Prof Michael S. Barr and Mr Alok Mittal for their engagement. We are especially grateful to Mr David Medine for his generosity with time and nuanced consideration of our views and questions. We would also like to thank Mr Greg Chen, Mr Karthik Viswanathan, and our legal team at TRA Law in particular Nehaa Chaudhari and Pushan Dwivedi.

aggregation technologies are capable of revealing sensitive information from the processing of seemingly non-sensitive personal data. Simultaneously, we propose that de-identified personal data should therefore *not* be caught by this future law i.e. if data is anonymised or otherwise de-identified it should not attract any obligations under a future regime.

3. **A test of "Legitimate purpose"** should be the primary grounds for processing data in each stage of the data life-cycle. Under this approach, personal data would only be collected, processed, shared or retained if this test was met. The test requires personal data use to be lawful, necessary for the provision of the good or service, and proportionate i.e. balanced against the rights of the individual. We have proposed some language for a test in Indian law on which we welcome comments and feedback (see our responses to Chapter 4, Part III of the White Paper).

4. **Consent:** While we propose that the test of legitimate purpose should be the primary ground for processing, consent should remain an important part of a future data protection regime. In our model, consent should only be requested if there is a legitimate purpose to collect the personal data in question. Consent and the associated privacy notice would then empower individuals and provide them with information regarding the use of their personal data, their various rights and an option to opt-out of the proposed use of their data.

5. **Individuals' data rights**: We propose that the future law should guarantee a bundle of rights to individuals. This would require entities to manage their data practices in a manner that is consistent with these rights. We propose that the future law should provide the following types of rights, as further described in our responses.

    i. Right to consent for collection of personal data
    ii. Right to processing for legitimate purposes only
    iii. Right to adequate data security
    iv. Right against disclosure of personal data
    v. Right to access personal data
    vi. Right to correction of personal data
    vii. Right to data portability
    viii. Rights related to automated decision making
    ix. Right against harm
    x. Right to informational privacy
    xi. Right to a clear, plain and understandable privacy notice
    xii. Right to privacy by design
    xiii. Right to breach notification

    An important proposal in our response is to provide individuals a right against harm and a right to informational privacy, which we expand upon in our responses.

6. **Responsive regulation**: The regulatory structure proposed is based on the theory of responsive regulation which is a dynamic and context sensitive regulatory framework. We also highlight the importance of *ex-ante* enforcement tools and incentives that can engender better data practice before a data breach occurs.

7. **Systemically important data entities**: Drawing from financial sector thinking, we propose entities **processing** personal data be categorised into systemically important data, normal risk and low risk

entities, based on the risk of harm they pose. A detailed methodology and framework should be created to operationalise this approach, taking into relevant factors in the context of data regulation. Such a gradation would allow future supervisory and enforcement activities to be better targeted in a complex data economy while state capacity continues to develop.

8. **Liability**: We propose a two tier liability model where (i) a strict liability standard for most well-defined obligations where these relate to conduct requirements set out by the law and fleshed out by regulation (ii) a reasonable efforts standard for entities to avoid causing harm or infringing informational privacy.

9. **Inter-sectoral Coordination:** An important aspect for data regulation to be successful in the future is inter-sectoral coordination. Such co-ordination between sectoral regulators and the regulator for data protection shall allow creation of specific and nuanced regulations for various sectors, improve supervision, reduce risk of regulatory arbitrage. We propose such co-ordination be achieved using tools for engagement such as suitable Memorandum of Understanding between the relevant regulators.

The White Paper raises key issues which are relevant to any data protection regime in the world. The questions it poses are at the frontiers of law, policy and regulation. We humbly submit our thinking on these issues as it currently stands, and look forward to continuing research to feed into a constructive national and global dialogue on these important questions.

We have listed our comments below, as against the corresponding questions numbered in accordance with the relevant sections across the various chapters and Parts of the White Paper. We have commented on select issues based on our areas of expertise. In this document, all questions raised by the White Paper are listed in blue text and our responses to those questions are in black text.

Contents

Part II of the White Paper (Scope and Exemptions)

Chapter 1: Territorial and Personal Scope

1. What are your views on what the territorial scope and the extra-territorial application of a data protection law in India?

We believe that any future data protection law must apply across the territory of India to all entities processing the personal data of individuals in India. In addition, the law must also apply to foreign entities processing the personal data of those in India in certain circumstances. This will be necessary to ensure that the rights of individuals are consistently protected across the market and various service providers they interact with. If foreign entities are not subject to the same obligations as Indian entities, it could also create anti-competitive effects by imposing different legal requirements on entities undertaking similar activities.

Accordingly, we propose that the future law should apply to an entity not established in India i.e. where the foreign entity:

- has a place of business in India by itself or through an agent, physically or through electronic mode and conducts business activity in India in any other manner; and
- is processing the personal data of individuals who are in India.

The first limb of this formulation borrows from the formulation under the Companies Act 2013 that applies that law to foreign companies (*see* the definition of "foreign company" under section 2(42) of the Companies Act, also reproduced for convenience in our response to question 3 under section 1.6, Part II of the White Paper). This approach would follow the formulation many entities already operating in India are already comfortable with. Several other key regulations in India, such as the Banking Regulation Act, 1949 and the Reserve Bank of India Act, 1934 also extend to foreign companies that undertake particular activities in India. This approach focusses on the conduct of business by these foreign entities offering goods and performing services in India, and therefore would not apply to foreign entities that do not operate in India.

The second limb of this formulation would ensure that the future law would apply to those foreign entities (including those not conducting business in India) that process the data of individuals present in India.

We should clarify that this means that foreign entities that *do not* collect or process personal data of individuals in India, but merely have an internet presence and appear to Indian users would not be subject to this law. This would avoid over-extension of jurisdiction, for instance by subjecting all websites to Indian law. Finally, we believe that this two-prong formulation would ensure that the requirements of the law also apply to entities that are purely foreign data processors i.e. processing personal data collected from India by a data controller with obligations under Indian law.

We believe this proposed approach will give the Indian law comprehensive jurisdiction that is compatible with other global data protection laws. This approach would also have the effect of incentivising entities (both local and foreign) to arrange their data practices in such a way as to avoid collecting and processing personal data where it is not relevant to their business.

2. To what extent should the law be applicable outside the territory of India in cases where data of Indian residents is processed by entities who do not have any presence in India?

As noted above, the future law should be applicable to foreign entities that conduct business activities in India and process the data of individuals present in India. The definition of "foreign companies" under the Companies Act 2013 is a well-understood in the Indian context and is a useful starting point on this issue.

3. While providing such protection, what kind of link or parameters or business activities should be considered?

Alternatives:

a. Cover cases where processing wholly or partly happens in India irrespective of the status of the entity.
b. Regulate entities which offer goods or services in India even though they may not have a presence in India (modelled on the EU GDPR)
c. Regulate entities that carry on business in India (modelled on Australian law), business meaning consistent and regular activity with the aim of profit.

The future law could consider the formulation in section 2(42) of Companies Act 2013 which defines a "foreign company" to whom that law applies as below:

> "*"foreign company" means any company or body corporate incorporated outside India which—*
> *(a) has a place of business in India whether by itself or through an agent, physically or through electronic mode; and*
> *(b) conducts any business activity in India in any other manner*."

We also propose that a future data protection law could capture all relevant entities that conduct business in India and collect personal data from those present in India, by defining the relevant entities to include a data controller or data processor that is:

- body corporate incorporated under any law for the time being in force in India; or
- a foreign company within the meaning of section 2(42) of Companies Act, 2013 (No. 18 of 2013).

4. What measures should be incorporated in the law to ensure effective compliance by foreign entities *inter alia* when adverse orders (civil or criminal) are issued against them?

5. Are there any other views on the territorial scope and the extra-territorial application of a data protection law in India, other than the ones considered above?

Chapter 2: Other Issues of Scope

1. What are your views on the issues relating to applicability of a data protection law in India in relation to: (i) natural/juristic person; (ii) public and private sector; and (iii) retrospective application of such law?

We agree with the provisional view of the Committee that the future data protection law should apply to solely natural persons. We also agree with the provisional view that the law must apply public sector and private sector entities. Exemptions, if any, should be limited and well-defined to ensure that the law does not become meaningless.

We further urge the Committee to recommend the application of the future law to *all* natural persons present in India, irrespective of whether they are citizens. As noted in our response to questions posed in section 1.6 under Part II of the White Paper, the rule of territorial nexus means that a country can make law to apply to matters within the territory of that country. It is important to note that this power of a country allows it to legislate for its own subjects and for foreigners within its jurisdiction (p281, Sarathi, 2005).

The approach of affording all persons in the territory of India protections and causes of actions would be in line with a vast number of Indian laws. Relevant instances of other Indian legislations which take this approach are listed below.

(i) The law that currently governs the handling of **personal data** in India—the Information Technology Act 2000, provides protections and compensation to *all* persons (without restricting this definition to citizens)[2].

(ii) The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 explicitly covers residents[3] of India who may not be citizens, entitling them as it does to obtain an Aadhaar number and providing protections (such as mandating confidentiality of all individuals' information[4]) under the Act.

(iii) The Consumer Protection Act 1986, which seeks to protect the interests of consumers buying goods or services in India, allows both Indian and foreign complainants to bring complaints against traders and service providers under the Act.

[2] See section 43A of the Information Technology Act, 2000 (as amended).
[3] Section S.3(1), the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016.
[4] Section 2(v), the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016.

(iv) In the **financial sector**, some key laws dealing with individuals' rights and personal information do not differentiate between citizens and non-citizens. The Credit Information Companies (Regulation) Act, 2005 applies to any "borrower"[5] or "client"[6] of a credit institution, defining the term widely to include any person in India. More recent legislation like the Insolvency and Bankruptcy Code 2016, which provides for the re-organisation and insolvency resolution of corporate persons, partnership firms and individuals, specifically includes provisions that apply to persons resident outside India.[7]

We also note the observation by Chandrachud, J in *K.S.Puttaswamy v. Union of India*[8] that the right to informational privacy (which will ostensibly be protected under the future data protection law) emerges "*primarily from the guarantee of life and personal liberty in Article 21 of the Constitution*" in addition to other guarantees under Part III (Fundamental Rights) of the Constitution of India. The Right to Life under Article 21 of the Indian Constitution itself applies to *all* persons[9],and has been interpreted to be all citizens, residents and foreigners in India[10].

This approach of granting protection to non-citizens is also being followed by other jurisdictions that are re-purposing their data protection laws. Notably, the EU's General Data Protection Regulation of 2016 affords protections to all "*natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data*"[11]. The Australian Privacy Act also protects the personal information of individuals who are physically within the border of Australia (Leonard, 2014). As a practical matter, entities it would be impossible for them to check the

[5] Section 2(b) of the Credit Information Companies (Regulation) Act, 2005 states*: ""borrower" means any person who has been granted loan or any other credit facility by a credit institution and includes a client of a credit institution"*."

[6] Section 2(c) of the Credit Information Companies (Regulation) Act, 2005 states:
""client" includes—
(i) a guarantor or a person who proposes to give guarantee or security for a borrower of a credit institution; or
(ii) a person—
(A) who has obtained or seeks to obtain financial assistance from a credit institution, by way of loans, advances, hire purchase, leasing facility, letter of credit, guarantee facility, venture capital assistance or by way of credit cards or in any other form or manner;
(B) who has raised or seeks to raise money by issue of security as defined in clause (h) of section 2 of the Securities Contracts (Regulation) Act, 1956 (42 of 1956), or by issue of commercial paper, depository receipt or any other instrument;
(C) whose financial standing has been assessed or is proposed to be assessed by a credit institution or any other person or institution as may, by notification, be directed by the Reserve Bank;"

[7] See sections 3(23), 3(24) and 3(25) of the Insolvency and Bankruptcy Code, 2016.

[8] (2017) 10 SCC 641

[9] Article 21, Constitution of India, 1950:
"*Protection of life and personal liberty: No person shall be deprived of his life or personal liberty except according to procedure established by law*".

[10] p16, A.M.Ahmadi, C.J., NHRC v. State of Arunachal Pradesh (1996) 1 SCC 742; p34, S.Saghir Ahmad, J., The Chairman, Railway Board v. Chandrima Das AIR 2000 SC 988; Anwar v. State of J&K ((1971) 3 SCC 104)).

[11] See Recital 14 of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016
on the protection of natural persons with regard to the processing of personal data and on the free
movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Available at <http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf>.

citizenship of individuals whose data they were collecting and treat the data accordingly. Data controllers and data processors under the future law will need to have data practices in line with their obligations uniformly across the board.

2. Should the law seek to protect data relating to juristic persons in addition to protecting personal data relating to individuals?

Alternatives:

a. The law could regulate personal data of natural persons alone.
b. The law could regulate data of natural persons and companies as in South Africa. However, this is rare as most data protection legislations protect data of natural persons alone.

We agree with the Committee's provisional view that the purpose of the future data protection law should be solely the protection of the personal data of identifiable natural persons. As the Committee notes, the South African position (that extends protections to juristic entities) is fairly unique. We understand that the South African position is also influenced by that country's constitutional jurisprudence which extends juristic persons rights under their Bill of Rights (South African Law Reform Commission, 2005). In India however, the protection of personal data has thus far been extended only to natural persons. This is the case under the Information Technology Act 2000 and related rules. The notion of informational privacy, a key imperative to establish a stronger data protection regime in India, is also which has become more well-defined in our own Constitutional tradition following the landmark judgement of a nine-judge Constitutional bench in *K.S.Puttaswamy v. Union of India* (2017). While holding that a fundamental right to privacy exists in India, the judges drew strongly on concepts of human dignity, individual liberty and individual autonomy. Seen in this light, the right to informational privacy appears to be tied firmly in to the human rights paradigm in India, and consequently related data protections should be given to natural persons.

3. Should the law be applicable to government/public and private entities processing data equally? If not, should there be a separate law to regulate government/public entities collecting data?

Alternatives:

a. Have a common law imposing obligations on Government and private bodies as is the case in most jurisdictions. Legitimate interests of the State can be protected through relevant exemptions and other provisions.
b. Have different laws defining obligations on the government and the private sector.

As noted in our response to question 1 posed in section 2.5 under Part II of the White Paper, we agree with the provisional view of the Committee that the law must apply public sector and private sector entities. Differing standards for public and private bodies would leave room for regulatory

arbitrage, especially where public and private sector entities operate side-by-side and provide similar services, for e.g. in the case of telecom. In any event, as more private sector actors are able to integrate and use public data infrastructure—as showcased by the Aadhaar & Indiastack system—it would be inconceivable to allow state and non-state actors to follow different standards of data protection.

We also reiterate that any exemptions from data protection obligations under the Act should be clearly defined and strictly interpreted to avoid making the law meaningless.

4. Should the law provide protection retrospectively? If yes, what should be the extent of retrospective application? Should the law apply in respect of lawful and fair processing of data collected prior to the enactment of the law?

Alternatives:

a. The law should be applicable retrospectively in respect of all obligations.
b. The law will apply to processes such as storing, sharing, etc. irrespective of when data was collected while some requirements such as grounds of processing may be relaxed for data collected in the past.

5. Should the law provide for a time period within which all regulated entities will have to comply with the provisions of the data protection law?

6. Are there any other views relating to the above concepts?

Chapter 3: Definition of personal data

1. What are your views on the contours of the definition of personal data or information?

We agree with the views of the Committee that personal data protected under the future data protection law should include *all* data, irrespective of form or accuracy. Our existing definition of "personal information" already contained in rule 2(i) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 is a strong definition which we can continue to use in India, and states that:

> "*"Personal Information" means any information that relates to a natural person which, either directly or indirectly, in combination with other information available or likely to be available is capable of identifying such person*".

This definition captures the core protection that is the objective of any data protection law i.e. to ensure that information by which an individual is **identified or identifiable** is not misused or used without their permission. In order to ensure that this core objective is upheld, it is necessary to afford protection to all personal information that relates to an identified natural person at the same level.

We propose that the future data protection law should have a single standard of data protections offered to all personal data of an individual. A "list based" approach, currently followed under the architecture of the Indian Informational Technology Act of 2000 (as amended) which categorises certain data as "sensitive" and therefore deserving of higher protections than other personal information in ineffective in the data economy of the 21st century. The old "list based" approach is ineffective for three key reasons:

1. We are currently seeing the generation of countless new types of data from individuals on a constant basis, several of which may not be contemplated by a static list of pre-determined "sensitive" data types yet be extremely sensitive for an individual.
2. Advances in data aggregation and mining techniques (so-called Big Data analytics) are capable of processing seemingly non-sensitive sets of information to reveal sensitive personal information about the person. This poses unsurmountable difficulties even for a well-informed individual when they are rationally selecting and sharing data, since it could be processed in a manner that reveals information that they do not want to reveal. It is possible to link information historically considered non-PII to specific individuals or devices and businesses actually have strong incentives to do so (US FCC, 2016).
3. The sensitivity of any data is very contextual. A variable which may not be sensitive in one context, could be highly sensitive in another. Hence, there is no objective way of determining whether a particular type of data is sensitive or not so, and is heavily dependent on context as jurists like Nissenbaum have pointed out. (Nissenbaum, 2004)

Jurisdictions including the United States have recognised the shortcomings of this list-based approach and shifting to a new approach that affords protection to all personally identifiable information.

It is important to note that under this approach, **de-identified data would not be the subject of the law**. Therefore, entities that use techniques like anonymisation or pseudonymisation (or other techniques which may arise in the future) to ensure that data no longer identifies an individual will not be caught by such a framework. Such an approach would incentivise the active use of anonymisation techniques and technologies in data practice by relevant entities.

Finally, the exemptions provided to the law for research, medical, personal and household and other relevant purposes (as the White Paper already notes) will ensure that those who genuinely need access to identifiable personal data can do so without the obligations that apply to other entities.

We therefore reiterate our submission that the future data protection law should apply to all personal data that serves to identify a natural person. The law should also extend to all forms of data irrespective of the form in which they are stored, i.e. by both physical or electronic means. The law should not apply to de-identified information, incentivising entities to use de-identification techniques (like anonymisation and pseudonymisation) thereby protecting the rights of individual data subjects as well as allowing a balance with legitimate purposes of companies. In conjunction with the exemptions that are already being proposed by the Committee, this approach will ensure that the law is not overbearing but in keeping with the foremost thinking around data regulation in our time.

2. For the purpose of a data protection law, should the term 'personal data' or 'personal information' be used?

Alternatives:

a. The SPDI Rules use the term sensitive personal information or data.
b. Adopt one term, personal data as in the EU GDPR or personal information as in Australia, Canada or South Africa.

The data protection law can use the term "personal data". The term should be clearly defined by the law as discussed in our response to the previous question.

3. What kind of data or information qualifies as personal data? Should it include any kind of information including facts, opinions or assessments irrespective of their accuracy?

Our previous responses in this section set out the definition of personal data that we propose to the Committee. In addition, we note that data which identifies a person, every if it is inaccurate must be covered by the law. Such data especially has the potential for harm to individuals precisely because of their inaccuracy. The law should provide individuals the right to access their data where it has been retained by entities, and specially provide rights to correct their own data.

4. Should the definition of personal data focus on identifiability of an individual? If yes, should it be limited to an 'identified', 'identifiable' or 'reasonably identifiable' individual?

As referred to our response to question 1 of section 2.5, Part II of the White Paper, any personal data which identifies or can identify an individual, either directly or in combination with other data, should be considered personal data. We should create an intermediate category of "reasonably identifiable" as this qualifier does not serve to either widen or narrow the category of information that will be caught by the law. It will only serve to introduce an unhelpful degree of subjectivity.

In our view, all de-identified data should be outside the purview of personal data since such data cannot reveal a specific individual and hence cause harm to the individual. Any techniques that can de-identify information should be encouraged.

A wide variety of techniques are available for the anonymisation of data, which may reduce the identifiability of individuals to various degrees. It must be recognised that these techniques are often vulnerable to techniques of de-anonymisation as well. Data anonymised today may become vulnerable to de-anonymisation at a later date so companies should make active efforts to keep personal data de-identified. (Raghunathan, 2013)

5. Should anonymised or pseudonymised data be outside the purview of personal data? Should the law recommend either anonymisation or psuedonymisation, for instance as the EU GDPR does?

[Anonymisation seeks to remove the identity of the individual from the data, while pseudonymisation seeks to disguise the identity of the individual from data. Anonymised data falls outside the scope of personal data in most data protection laws while psuedonymised data continues to be personal data. The EU GDPR actively recommends psuedonymisation of data.]

6. Should there be a differentiated level of protection for data where an individual is identified when compared to data where an individual may be identifiable or reasonably identifiable? What would be the standards of determining whether a person may or may not be identified on the basis of certain data?

We propose that a statutory strict liability should apply for the contravention of obligations when entities are processing personal data. Please see our responses to Part IV, section 2.5 of the White Paper which detail our responses on this matter.

7. Are there any other views on the scope of the terms 'personal data' and 'personal information', which have not been considered?

Chapter 4: Definition of Sensitive Personal Data

1. What are your views on sensitive personal data?

In our view, the law should not classify a particular set of data types to be sensitive personal data and accord them a higher level of data protection. Please refer to our response to question 1, Chapter 3 of Part II of the White Paper.

To reiterate the reasons why the list-based approach does not work:

1. countless new types of data are being generated about individuals on a constant basis, several of which may not be contemplated by a static list of pre-determined "sensitive" data;
2. advances in data aggregation and mining techniques (so-called Big Data analytics) are capable of processing seemingly non-sensitive sets of information to reveal sensitive personal information about the person, and
3. the sensitivity of any data is heavily contextual.

Just as subjectivity in the determination of sensitivity varies across contexts, it also varies across time – as evidenced from the difficulties we currently face with the list of sensitive personal data included in the Indian law.

2. Should the law define a set of information as sensitive data? If yes, what category of data should be included in it? Eg. Financial Information / Health Information / Caste / Religion / Sexual Orientation. Should any other category be included? [For instance, the EU GDPR incorporates racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life.]

As mentioned in our response to the previous question, no specific set of data types should be defined as sensitive. All personal data should enjoy same level of data protection.

3. Are there any other views on sensitive personal data which have not been considered above?

Chapter 5: Definition of Processing

1. What are your views on the nature and scope of data processing activities?

In our view, all activities that may be carried out on personal data during its entire life-cycle from collection to its destruction should be covered within the scope of data processing in the data protection law. We agree with the view of the Committee that the law should not attempt to provide a complete list of operations that collectively form processing considering the continuously changing world of data processing. To this effect, we propose the following definition of "processing":

> *"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."*

This approach will allow the proposed law to provide for broad coverage of different activities that are already being carried out by entities today while also ensuring that any newer types of activities which may be developed in the future remain within its purview.

2. Should the definition of processing list only main operations of processing i.e. collection, use and disclosure of data, and inclusively cover all possible operations on data?

To reiterate, we think that the ambit of processing is broader than the functions of collection, use, disclosure of data. The definition used in the future data protection law should include all operations involved in the chain of processing personal data. To this effect, we have proposed a definition in response to question 1 in section 5.4 of the White Paper, above.

3. Should the scope of the law include both automated and manual processing? Should the law apply to manual processing only when such data is intended to be stored in a filing system or in some similar structured format?

Alternatives:

a. All personal data processed must be included, howsoever it may be processed.
b. If data is collected manually, only filing systems should be covered as the risk of profiling is lower in other cases.
c. Limit the scope to automated or digital records only.

The future data protection law should apply to both automated and manual processing of personal data. Additionally, the law should be applicable to all personal data collected manually and not offer selective protection to particular formats. Given that continuous improvement in technology is making it increasingly easier to digitize manually stored data, the proposed law should provide for same standards for processing of data, regardless of its form (digital or manual), format (structured or unstructured) or the currently perceived ease of profiling.

4. Are there any other issues relating to the processing of personal data which have not been considered?

Chapter 6: Definition of Data Controller and Processor

1. What are your views on the obligations to be placed on various entities within the data ecosystem?

As the White Paper has recognised, in today's world of globalisation and out-sourcing a wide variety of entities are found within the ecosystem which is involved in the processing of personal data. These entities do not exercise the same level of control over the personal data being

processed. The levels of technical expertise and involvement in various data processes are also likely to vary quite widely amongst the entities in the ecosystem (Alsenoy, 2017). Accordingly, in our view, the obligations placed on various entities processing data should be in line with their place in ecosystem. Such a model of allocating responsibility will help in ensuring the following:

i. maximum positive effect of the regulations, i.e. the highest level of privacy data security for the personal data being processed.
ii. minimisation of the cost of compliance with regulations while ensuring adequate levels of privacy and security for personal data.
iii. enforceability of the regulations. (EU Data Protection Working Party, 2010)

2. Should the law only define 'data controller' or should it additionally define 'data processor'?

Alternatives:

a. Do not use the concept of data controller/processor; all entities falling within the ambit of the law are equally accountable.
b. Use the concept of 'data controller' (entity that determines the purpose of collection of information) and attribute primary responsibility for privacy to it.
c. Use the two concepts of 'data controller' and 'data processor' (entity that receives information) to distribute primary and secondary responsibility for privacy.

Among the above outlined alternatives, the third alternative is most suitable. The law should clearly define both 'data controller' and 'data processor', which would help create a broad categorisation among the entities making up the data ecosystem. Such a categorisation shall enable the allocation of different obligations to the different types of entities that make up the data ecosystem. We have presented our proposal for how such entities can be defined for clarity in response to question 3 below posed in section 6.4, Part II of the White Paper.

Apart from enabling the allocation of responsibility, clearly defining the different entities will also clarify liability and ease the burden of proof in case of a failure to meet the obligations laid out in the law. On a related point, we also note the high level of difficulty a data subject would have in pin-pointing and proving which entity in a chain was responsible for the act or omission which resulted in the contravention of data protection obligations. Accordingly, we propose that where an individual establishes *prima facie* that an entity's act or omission has resulted in a violation of their rights under the future law, the burden of proof should shift to the entities in the chain to prove that it did not commit or was not responsible for the commission of the acts or omissions in question.

We also note that the other alternatives noted in this question are not suited for the future regime. Alternative 'a' above will increase the overall cost of compliance while also creating confusion regarding which of the many entities making up the data ecosystem are in fact responsible for meeting a particular provision in the law. Meanwhile alternative 'b', it would place excessive burden on the controllers even in situations where

the controller is not best placed to ensure compliance with regulations, which can result in situation where personal data does not enjoy an adequate level of protection.

3. How should responsibility among different entities involved in the processing of data be distributed?

Alternatives:

a. Making data controllers key owner and making them accountable.
b. Clear bifurcation of roles and associated expectations from various entities.
c. Defining liability conditions for primary and secondary owners of personal data.
d. Dictating terms/clauses for data protection in the contracts signed between them.
e. Use of contractual law for providing protection to data subject from data processor.

In our view, "data controllers" should remain primarily responsible for compliance with all regulations outlined in the law. At the same time, as outlined in our response to Question 1 above, both primary and secondary owners of the data should have clearly defined responsibilities. Thus, the law should clearly define liability conditions according to the obligations that the law places on both 'data controllers' and 'data processors'.

In our view, data controllers should be defined as

> *""data controller" means the natural or legal person which, alone or jointly with others, (1) determines the purposes and means of the processing of personal data or (2) collects personal data from an individual prior to or during the performance or provision of a service or product, or when entering into a contract;"*

Data processors should be defined as

> *""data processor" means natural or legal person which processes personal data on behalf of the controller*;"

The law should also clearly assign responsibilities to both data controllers and data processors with provisions like,

> *'Any transfer of personal data to a third country shall take place only if the data controller or data processor has ensured that appropriate and enforceable safeguards with effective legal remedies for individuals are available.'*

The above provision places an obligation on both data controllers as well as data processors to ensure the privacy and security of personal data before allowing for cross-border transfer of such data. Such a provision places an additional responsibility on data processors that are likely to be in a better place to evaluate whether adequate safeguards are available or not.

Such provisions will create a comprehensive framework of obligations that the law shall place on different entities making up the data ecosystem using personal data. We believe this combination of specific definitions of different types of entities making up the data ecosystem and clear distribution of responsibilities among them will help in achieving the goals laid out in our response to question 1 above.

4. Are there any other views on data controllers or processors which have not been considered above?

Apart from the above, we would also like to highlight the following two views with respect to the entities making up the data ecosystem.

i. We have the view that in cases where there are multiple entities having status of joint controllers, the liability of failure to meet with the regulations should be 'joint and several' in nature.

   With the emergence of new technologies, we are likely to encounter situations where there are multiple controllers of the personal data being processed. In such a situation it may become difficult to clearly assign responsibility for a particular failure in the compliance with the regulations laid out in the law. In addition, it is also unlikely that the data subject to be able to reasonably determine the specific controller liable for the failure. Thus, to strengthen the enforceability of the law the liability of failure should be 'joint and several'.

ii. We agree with the provisional views of the committee that the test for 'data controller' status of an entity, as is reflected in the definition of 'data controller' given in our response to the previous question. While a large number of entities are often involved in the overall processing of personal data, only some of them are the actual decision makers, i.e. entities that decide on the 'why' and 'how' of data processing. These entities have a much higher level of influence over the processing of personal data compared to other entities in the ecosystem and, in our view, should be held responsible accordingly. (UK Information Commisioner's Office, 2014)

We are in favour of also including another class of entities within the data ecosystem into the ranks of 'data controllers'. Considering the limited exposure to and understanding of modern technologies among a large section of the Indian population, we are of the view that entities which are directly involved in interacting with the 'data subjects' should be considered as data controllers and hence have overall responsibility of ensuring adequate informational privacy of the subjects.

Chapter 7: Exemptions

1. What are the categories of exemptions that can be incorporated in the data protection law?

2. What are the basic security safeguards/organisational measures which should be prescribed when processing is carried out on an exempted ground, if any?

Domestic /Household Processing

1. What are your views on including domestic/household processing as an exemption?

2. What are the scope of activities that will be included under this exemption?

3. Can terms such as ‘domestic’ or ‘household purpose‘ be defined?

4. Are there any other views on this exemption?

Journalistic/Artistic/ Literary Purpose

1. What are your views on including journalistic/artistic/literary purpose as an exemption?

2. Should exemptions for journalistic purpose be included? If so, what should be their scope?

3. Can terms such as ‘journalist’ and ‘journalistic purpose’ be defined?

4. Would these activities also include publishing of information by non-media organisations?

5. What would be the scope of activities included for ‘literary’ or ‘artistic‘ purpose? Should the terms be defined broadly?

6. Are there any other views on this exemption?

Research/Historical/Statistical Purpose

1. What are your views on including research/historical/statistical purpose as an exemption?

2. Can there be measures incorporated in the law to exclude activities under this head which are not being conducted for a bonafide purpose?

3. Will the exemption fail to operate if the research conducted in these areas is subsequently published/ or used for a commercial purpose?

4. Are there any other views on this exemption?

Investigation and Detection of Crime, National Security

1. What are your views on including investigation and detection of crimes and national security as exemptions?

2. What should be the width of the exemption provided for investigation and detection of crime? Should there be a prior judicial approval mechanism before invoking such a clause?

3. What constitutes a reasonable exemption on the basis of national security? Should other related grounds such as maintenance of public order or security of State be also grounds for exemptions under the law?

4. Should there be a review mechanism after processing information under this exemption? What should the review mechanism entail?

5. How can the enforcement mechanisms under the proposed law monitor/control processing of personal data under this exemption?

6. Do we need to define obligations of law enforcement agencies to protect personal data in their possession?

7. Can the Data Protection Authority or/and a third-party challenge processing covered under this exemption?

8. What other measures can be taken in order to ensure that this exemption is used for bona fide purposes?

9. Are there any other views on these exemptions?

Additional Exemptions

1. Should ‘prevention of crime’ be separately included as ground for exemption?

2. Should a separate exemption for assessment and collection of tax in accordance with the relevant statutes be included?

3. Are there any other categories of information which should be exempt from the ambit of a data protection law?

Chapter 8: Cross Border Flow of Data

1. What are your views on cross-border transfer of data?

2. Should the data protection law have specific provisions facilitating cross border transfer of data? If yes, should the adequacy standard be the threshold test for transfer of data?

3. Should certain types of sensitive personal information be prohibited from being transferred outside India even if it fulfils the test for transfer?

4. Are there any other views which have not been considered?

Chapter 9: Data Localisation

1. What are your views on data localisation?

2. Should there be a data localisation requirement for the storage of personal data within the jurisdiction of India?

3. If yes, what should be the scope of the localisation mandate? Should it include all personal information or only sensitive personal information?

4. If the data protection law calls for localisation, what would be impact on industry and other sectors?

5. Are there any other issues or concerns regarding data localisation which have not been considered above?

Chapter 10: Allied Laws

Currently, there are a variety of laws in India which contain provisions dealing with the processing of data, which includes personal data as well as sensitive personal data. These laws operate in various sectors, such as, the financial sector, health sector and the information technology sector. Consequently, such laws may need to be examined against a new data protection legal and regulatory framework as and when such framework comes into existence in India.

Taking into account our expertise and field of operation, we are limiting our response in this chapter to laws are regulations of the financial sector.

In our view, within the financial sector the following sections of the respective laws/regulations need to examined and appropriately reconciled with the provision of the data protection law.

- Prevention of Money Laundering Act, 2002 (PMLA)
- Payments and Settlement Systems Act, 2007
- RBI KYC Master Direction, 2016
- RBI Charter of Customer Rights
- RBI Master Circular on Credit Card, Debit Card and Rupee Denominated Co-branded Pre-paid Card Operations of Banks and Credit Card issuing NBFCs
- RBI Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks and NBFCs
- Regulations Issued under SEBI Act 1992
- Regulations issued by IRDAI under the Insurance Act, 1938
- Regulations issued by PFRDA under the PFRDA Act, 2013
- Credit Information Companies Rules 2006

It must be noted that the list of regulations or laws given in the White paper does not include the Prevention of Money Laundering Act of 2007 and also regulations issued by the Pension Fund Regulatory and Development Authority.

Prevention of Money Laundering Act, 2002

Under Section 12(1) of the PMLA, every reporting entity is required to verify the identity of its clients, maintain a record of documents evidencing the identity of its clients, maintain a record of transactions so as to enable it to reconstruct individual transactions, etc. In the context of

confidentiality obligations, per Section 12(2) of PMLA, every reporting entity (which includes banks, financial institutions, intermediaries, etc.) is under an obligation to keep confidential every information maintained, furnished or verified, save as otherwise provided under any law for the time being in force. Thus, client/ customer confidentiality is required to be maintained by all reporting entities covered under the PMLA.

In our view, this provision of the PMLA should not be in contravention of any provision in the data protection law.

Payments and Settlement Systems Act, 2007

As per Section 22(1) of PSSA, a system provider shall not disclose to any other person the existence or contents of any document or part thereof or other information given to him by a system participant, except where such disclosure is required under the provisions of the PSSA or the disclosure is made with the express or implied consent of the system participant concerned or where such disclosure is in obedience to the orders passed by a court of competent jurisdiction or a statutory authority in exercise of the powers conferred by a statute.

In our view, the data protection law should result in reinforcement of the obligation to keep information collected by the payment system. While the regulation allows for disclosure of information with consent, any such disclosure should not override any of the rights of the individuals with regard to protection of their personal data given by the data protection law.

Also, as payment and settlement systems will have to interact with other financial service providers like banks they may act as data processors with respect to customer data that may be shared by banks or other financial service providers acting as data controllers. In this regard, there may be certain additional obligations that the data protection laws shall impose on payment systems.

RBI Charter of Customer Rights

The RBI Charter of Customer Rights dated December 3, 2014 provides in the context of protection of rights of bank customers, inter alia, that customers' personal information should be kept confidential unless they have offered specific consent to the financial services provider or such information is required to be provided under the law or it is provided for a mandated business purpose (for e.g., to credit information companies). It must be noted here that this charter is only applicable to banks regulated by the RBI and not to other NBFCs, Pre-paid Instrument issuing companies etc.

This obligation, in our view, is very much in line with the principles of data protection. At the same time, care must be taken by banks, as 'data controllers' under the data protection law, that all rights of bank customers guaranteed by the data protection law are also protected.

RBI Master Circular on Customer Service in Banks

The RBI Master Circular on Customer Service in Banks dated July 1, 2015 (Customer Service Circular) notes that the banks' obligation to maintain secrecy of information provided by the customer arises out of the contractual relationship between the bank and customer. This has been reiterated in the KYC Master Directions as well. The Customer Service Circular also mentions that wherever banks desire to collect any information about the customer for a purpose other than KYC requirements, it should not form part of the account opening form. Such information may be collected separately, purely on a voluntary basis, after explaining the objectives to the customer and taking his express approval for the specific uses to which such information could be put.

The Customer Service Circular also provides that no information should be divulged to third parties except under the following circumstances:

(a) where disclosure is under compulsion of law;

(b) where there is duty to the public to disclose;

(c) where interest of bank requires disclosure; and

(d) where the disclosure is made with the express or implied consent of the customer.

These regulations uphold the principles of data protection. The regulation also makes it clear that only data required to fulfil KYC requirements is mandatory, while all other data must be obtained on voluntary basis. This is in line with the principle of minimising the volume of personal data that should be collected to that which is necessary for the fulfilment of the good/service being provided. In our view, these regulations should not be in contravention with any provisions of the data protection law.

RBI Master Directions on Know Your Customer

The RBI Master Directions on Know Your Customer dated February 25, 2016 (KYC Master Directions) apply to every entity regulated by RBI including, *inter alia*, banks, non-banking financial companies, payment system providers, payment system participants, PPI issuers, etc. According to the KYC Master Directions, these entities are required to treat the information collected from customers for the purpose of opening of account as confidential and cannot divulge such details for the purpose of cross selling or for any other purpose without the express permission of the customer.

Per the KYC Master Directions, while considering the requests for data/ information from Government and other agencies, banks are required to satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the banking transactions. The only exceptions to such sharing of information are:

(a) where there is a duty to the public to disclose;

(b) where the interest of bank requires disclosure; and

(c) where the disclosure is made with the express or implied consent of the customer.

These regulations are largely in line with those provided by the RBI Customer Service Circular referred to above. As with those regulations, in our view the KYC Master Directions should not require any reconcilement with the data protection law.

RBI Master Circular on Credit Card, Debit Card and Rupee Denominated Co-branded Pre-paid Card Operations of Banks and Credit Card issuing NBFCs

Per the RBI Master Circular on Credit Card, Debit Card and Rupee Denominated Co-branded Pre-paid Card Operations of Banks and Credit Card issuing NBFCs dated July 1, 2015 (Card Master Circular), the card issuing bank/ NBFC are under an obligation to not reveal any customer information obtained at the time of opening the account or issuing the credit card to any other person or organization without obtaining their specific consent, as regards the purpose/s for which the information will be used and the organizations with whom the information will be shared. The application form for credit card is required to explicitly provide for consent the same. The information being sought from customers should not be of such nature as will violate the provisions of the laws relating to secrecy in the transactions.
Additionally, per the Card Master Circular, the card issuing bank should not reveal any information relating to customers obtained at the time of opening the account or issuing the card and the co-branding non-banking entity should not be permitted to access any details of customer's accounts that may violate the bank's secrecy obligations.

As with other regulations issued by the RBI, these obligations should also be in line with the provisions of the data protection law.

RBI Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks

The RBI Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks dated November 3, 2006 (Bank OS Guidelines) say that banks would be responsible for the actions of their service provider[12] and the confidentiality of customer information that is available with the service provider. The Bank OS Guidelines are applicable to outsourcing arrangements entered into by a bank with a service provider (who may be a member of the group/ conglomerate to which the bank belongs, or an unrelated party) located in India or elsewhere. The outsourcing agreements with the service providers should provide that confidentiality of customer's information should be maintained even after such agreement expires or gets terminated. The bank should seek to ensure the preservation and protection of the security and confidentiality of customer information in the custody or possession of the service provider. The bank should ensure that the service provider is able to isolate and clearly identify the bank's customer information, documents, records and assets to protect the confidentiality of the information.

Apart from the above broader guidelines regarding maintaining the confidentiality of customer data being handled by the service provider, the Bank OS Guidelines also include the following two obligations related to protection of customers' personal data.

i. The bank should review and monitor the security practices and control processes of the service provider on a regular basis and require the service provider to disclose security breaches**.**

ii. The bank should immediately notify RBI in the event of any breach of security and leakage of confidential customer related information. In these eventualities, the bank would be liable to its customers for any damage.

Once the data protection law comes into force, the relationship between the bank and its service providers will be considered as a relationship between a data controller and data processor. Whether the third party service provider is a data controller or data processor will depend on the definitions of these entities as per the data protection law. The proposed data protection law will accordingly impose certain obligations on both the bank and third party service provider. These obligations may not be in alignment with the obligations that the Bank OS Guidelines as outlined above. For example, the above guidelines lay the primary responsibility of data protection on the bank, i.e. the data controller. In our view, the data protection law should also impose certain specific obligation on data processors as well. The data protection law would then impose specific obligations on the third party service provider to whom the bank has outsourced certain activities. In the instance of the third party service provider being classified as data controller as well, all the obligations laid out in the data protection law are likely to apply.

[12] Service providers include direct sales agents/ direct marketing agents and recovery agents.

Hence, in our view, the RBI may need to put out a modified set of guidelines to regulate the relationship between banks and their service providers which are in line with the provisions of the data protection law.

Regulations under the SEBI Act, 1992

In 17 different sets of regulations issued by the Securities and Exchange Board of India include a specific obligation to maintain confidentiality of the data. Eight sets of regulation include specifics regarding situations where the data may be shared. The following table lists out these regulations including the specific regulation in question.

In 11 cases, the SEBI has prescribed a "code of conduct approach" where they have imposed a duty of confidentiality whereby the regulated/ licensed entity is required to abide by a code of conduct which is stipulated in the specific regulations. The key obligations imposed on the registered entity in this approach are: (i) maintenance of confidentiality; (ii) prohibition on divulging to anybody either orally or in writing, directly or indirectly, any confidential information about its clients which has come to its knowledge, without taking prior permission of its clients, except where such disclosures are required to be made in compliance with any law for the time being in force; (iii) unless otherwise required by law, maintenance of confidentiality and prohibition on divulging/ disclosing any information obtained in the discharge of their duty and prohibition on the use of such information for personal gains.

In 3 sets of regulations, i.e. Securities and Exchange Board of India (Custodian of Securities) Regulations, 1996, the Securities and Exchange Board of India (Foreign Portfolio Investors) Regulations, 2014, the Securities and Exchange Board of India (Research Analysts) Regulations, 2014, the obligation to maintain confidentiality of data is built into the main framework.

In our view, these obligations on maintenance of confidentiality should not conflict with the obligations imposed by the data protection law in regard to the personal data that are held by the intermediaries regulated by SEBI.

S. No.	Regulations	Confidentiality obligations	Data sharing provisions
1.	SEBI (Stock Brokers and Sub-Brokers), 1992	Please refer to Regulation 15 (3) and 7 (3)	Same as Regulation 15 (3) and 7 (3)
2.	SEBI (Merchant Bankers) Regulations, 1992	Please refer to regulation 15	Same as Regulation 15
3.	SEBI (Portfolio Managers) Regulations,	Please refer to Schedule III, Regulation	--

S. No.	Regulations	Confidentiality obligations	Data sharing provisions
	1993	13 (6),(7) and (10)(1)(c)	
4.	SEBI (Registrars to an issue and Share Transfer Agents) Regulations, 1993	Please refer to Schedule III, Regulation 13 (13), (27) and (31)(c)	Same as Regulation 13
5.	SEBI (Underwriters) Regulations, 1993	Please refer to Schedule III, Regulation 13 (10) and (21)	--
6.	SEBI (Debenture Trustees) Regulations, 1993	Please refer to Regulations 8 and 30	Same as Regulation 8
7.	SEBI (Bankers to an Issue) Regulations, 1994	Please refer to Regulation 11, 27, 16 (5)	Same as Regulation 11
8.	SEBI (Depositories and Participants) Regulations, 1996	Please refer to Fourth Schedule – Part A (v) (d), Fourth Schedule – Part B (ix) (b) and (c)	--
9.	SEBI (Custodian of Securities) Regulations, 1996	Please refer to Regulation 5, 19(1)(a), 17(b)(c)(d)(e)(f)(g), 17(2)(l) and (3) (l)	--
10.	SEBI (Credit Rating Agencies) Regulations, 1999	Please refer to Regulation 23, 15 and 19	Same as Regulation 23
11.	SEBI (Public Offer and Listing of Securitised Debt Instruments) Regulations, 2008	Please refer to Regulations 3(p) (vi) and 13	Same as Regulation 13
12.	SEBI (Intermediaries) Regulations, 2008	Please refer to Regulation 4	--
13.	SEBI {KYC (KRA) Registration Agency} Regulations, 2011	Please refer to Regulation 6 and 22.	Same as Regulation 6
14.	Securities Contracts (Regulation) (Stock Exchanges And Clearing Corporations) Regulations, 2012	Please refer to Schedule II – Part A(v)(d) and Schedule II – Part B (ix)(a),(b) and (c)	--
15.	SEBI (Investment Advisers) Regulations, 2013	Please refer to Regulations 9, 15(6) and 15(9)	--
16.	SEBI (Foreign Portfolio Investors)	Please refer to Regulation 3	--

S. No.	Regulations	Confidentiality obligations	Data sharing provisions
	Regulations, 2014		
17.	SEBI (Research Analysts) Regulations, 2014	Please refer to Regulation 5	--
18.	SEBI (Collective Investment Schemes) Regulations, 1999	Please refer to Regulation 40(2)	--

Apart from the above regulations, the SEBI Guidelines on Outsourcing of Activities also outline certain obligations that the SEBI registered intermediaries must comply with. The key obligations under these regulations are:

i. Outsourcing relationships between the intermediary and each third party shall be governed by written contracts/ agreements/ terms and conditions that is required to contain unambiguous confidentiality clauses to ensure protection of proprietary and customer data during the tenure of the contract and also after the expiry of the contract.
ii. The intermediary shall take appropriate steps to require that third parties protect confidential information of both the intermediary and its customers from intentional or inadvertent disclosure to unauthorized persons.

As in the case of the Bank OS Guidelines, the intermediary and the third party to whom they outsource activities will be considered data controller or data processor according to the respective definitions. Hence, we believe, the SEBI Outsourcing Guidelines may need to be reconciled with the obligations that shall be placed by the data protection law on these entities. For example, the data protection law, in our view, should directly impose obligation on data processors to safeguard the personal data. Hence, the third party, even if classified as a data processor, will have obligations of data protection directly imposed on them.

Regulations issued by Insurance Regulatory Authority of India

A specific obligation to maintain confidentiality has been included in 9 regulations issued by the IRDAI, while in 2 regulations specific contours on data sharing have been included. In 5 cases, the IRDAI has prescribed a "code of conduct approach" whereby the regulated/ licensed entity is required to abide by a code of conduct which is stipulated in the specific regulations. In 1 case, specific regulations issued by the IRDAI prescribe the obligation of confidentiality within its main framework (and not in the code of conduct) or in 3 cases both, within the framework as well as through the code of conduct. The following table lists these regulations, along with the specific provisions where they have been included.

These regulations mandate that regulated entities are obligated to: (i) treat all information supplied by the prospective clients/ prospects as completely confidential to themselves and to the insurer(s) to which the business is being offered; (ii) take appropriate steps to maintain the security of confidential documents in their possession.

Apart from the above two obligations, for certain regulations additional obligation are also placed. For example the IRDAI (Insurance Surveyors and Loss Assessors) Regulations, 2015 imposes an additional obligation to neither use nor appear to use, any confidential information acquired or received by him in the course of his professional work, to his personal advantage or for the advantage of a third party.

The data confidentiality obligations put by the IRDAI through their regulations are similar to those put by the RBI and SEBI. In our view, they should not require any changes to align with the data protection law.

S. No.	Regulations	Confidentiality obligations	Data sharing provisions
1.	IRDAI (Insurance Brokers) Regulations, 2013	Please refer to Regulation 28 and Regulation 2(d) and (e).	--
2.	IRDAI (Web Aggregators) Regulations, 2013	Please refer to Schedule VII (a)(iii)-(iv) and Schedule X (6)(b)(v)	--
3.	Revised Guidelines On Insurance Repositories and Electronic Issuance of Insurance Policies, 2015	Please refer to regulation 34.	--
4.	IRDAI (Registration Of Insurance Marketing Firm) Regulations, 2015	Please refer to Part II (c).	--
5.	IRDAI (Third Party Administrators - Health Services) Regulations, 2016	Please refer to Regulation 19 and Schedule II (2)(n).	Please refer to Regulation 19 (4) for data sharing
6.	IRDAI (Insurance Surveyors And Loss Assessors) Regulations, 2015	Please refer to Regulation 13 (1)(c) and Chapter VI (16) and (17)	Please refer to Regulation 16(16)
7.	IRDAI (Insurance Services By Common Service Centres) Regulations, 2015	Please refer to Schedule IV (I) (Regulation 4.2 and 14.9) and (2)(d) and (e) and (II) (Regulation 14.9) (5).	--

S. No.	Regulations	Confidentiality obligations	Data sharing provisions
8.	IRDAI (Licensing of Banks as Insurance Brokers) Regulations, 2013	Please refer to Schedule II (2)(d) and (e)	--
9.	IRDAI (Lloyd's India) Regulations, 2016	--	--
10.	IRDAI (Registration and Operations of Branch Offices of Foreign Reinsurers other than Lloyd's) Regulations, 2015	--	--
11.	IRDAI (Registration of Corporate Agents) Regulations, 2015	--	--

The obligation to maintain confidentiality of customer continues when the insurer outsources their activities to a third party. As per the Guidelines on Outsourcing of Insurance Activities dated February 1, 2011, the insurer is required to take appropriate steps to require that third party service providers protect confidential information of both the insurer and its clients from intentional or inadvertent disclosure to unauthorized persons. Apart from this the guidelines also mandate that any outsourcing of data storage must be with repository service providers authorized by the IRDAI. In this case as well, the guidelines for outsourcing may need to be modified since the insurance provider and any third party they outsource activities to will be considered as data controllers or data processors as per the provisions of the data protection law.

Regulations issued by the Pension Fund Regulatory and Development Authority

Specific obligations on maintaining confidentiality have been included in 11 regulations issued by the PFRDA and specific contours on data sharing have been included in 6 cases. In the case of 11 regulations, the PFRDA include obligations to maintain confidentiality of data within the main framework of the regulations. For 6 regulations, such obligation is included within a code of conduct and for 3 regulations such obligations can be found both within the prescribed code of conduct as well as the main regulations. The table below lists all the regulations issued by the PFRDA which include such obligations.

The obligation to maintain confidentiality referred to in the regulations issued by PFRDA broadly includes the following:

i. Obligation to not divulge to anybody, either orally or in writing, directly or indirectly, any confidential information about PFRDA, National Pension System Trusts or subscribers, which has come to their knowledge, without taking prior permission of PFRDA or National Pension System Trusts except where such disclosures are required to be made in compliance with any law for the time being in force;

ii. Obligation to seek from its prospects or subscribers, information about their financial situation, investment experience and retirement objectives relevant to the services to be provided and maintain confidentiality of such information; and

iii. General obligation to maintain confidentiality of information of the subscribers under the relevant scheme.

The above guidelines provide a broad obligation to pension fund providers to maintain confidentiality of the data that they collect from their prospects and subscribers. The guidelines also indicate the kind of information that may be collected and are relevant to the services that shall be provided. These guidelines, in our view should remain in line with the provisions of the contours of the data protection law.

S. No.	Regulations	Confidentiality obligations	Data sharing provisions
1.	PFRDA (Aggregator) Regulations, 2015	Please refer to regulation 40	Please refer to regulation 6 (1), Schedule VI (2)(a) and (b) and (3)(a), (b), (c) and (d)
2.	PFRDA (Custodian of Securities) Regulations, 2015	Please refer to regulation 11.	Please refer to the Fourth Schedule, III (3.4)
3.	PFRDA (Pension Fund) Regulations, 2015	Please refer to regulation 12 (12)	Please refer to Schedule VI (3.4)
4.	PFRDA (Retirement Adviser) Regulations, 2016	Please refer to regulation 18 (xii) Please refer to Schedule III (4)	--
5.	PFRDA (Point of Presence) Regulations, 2015	Please refer to regulation 42 and Schedule III (2)(a) and (b)	Please refer to regulation 3 (a), (b), (c) and (d)
6.	PFRDA (Trustee Bank) Regulations, 2015	Please refer to regulation 38	Please refer to Schedule I (d)
7.	PFRDA (Exits and Withdrawals	Please refer to regulation 38	--

S. No.	Regulations	Confidentiality obligations	Data sharing provisions
	under the National Pension System) Regulations 2015		
8.	PFRDA (Redressal of Subscriber Grievance) Regulations, 2015	Please refer to regulation 23 (2)	--
9.	PFRDA (National Pension System Trust) Regulations, 2015	Please refer to regulation 4(2)(a) and (h), regulation 38, Schedule III (10)	--
10.	PFRDA (Employees' Service) Regulations 2015	Please refer to regulation 50 (1), (2), (3) and (4).	--
11.	PFRDA (Central Record Keeping Agency) Regulations, 2015	Please refer to regulation 18(2)(l), regulation 43, Schedule III (11)	Please refer to Schedule III (4)

Credit Information Companies Rules 2006

According to Rule 28(2)(ii) of the Credit Information Companies Rules, 2006 (CIC Rules), every credit institution, CIC and specified user[13] is required to ensure that access to the data, information and credit information maintained by them is permitted only their managers or employees or designated officers, who are duly authorised for the purpose on a need to know basis. The CIC Rules do not specifically permit any credit institution or the specified user to authorize any other entity/ person as their agent to access the credit information of customers.

Apart from credit institutions, CICs and specified users, RBI Circular on Free Annual Credit Report to Individuals dated September 1, 2016 provides that CICs should provide access in electronic format, upon request and after due authentication of the requester, to one free full credit report including credit score, once in a year (January- December), to individuals whose credit history is available with the CIC.

The current obligations imposed on CICs maintain a high level of data protection as the data contained in the credit information reports are only allowed to be shared with certain authorised personnel who have a specific use of the data. Similarly, the data collected by the CICs are collected from other credit institutions or specified users with explicit consent of the customers of those entities. This should not be in contravention of any provisions in the data protection law.

[13] The CIC Act defines a specified user to mean any credit institution, CIC being a member of another CIC, and includes such other person or institution as may be specified by regulations made, from time to time, by the RBI for the purpose of obtaining credit information from a CIC.

In our view, the data protection law should provide every individual access to the personal data, generated by or associated with them, that is held by any entity. The RBI Circular on annual credit report combined with Rule 28(2)(ii) only authorised personnel in effect limits an individual's access to his/her own personal data that is being handled by CICs, including their credit scores generated. The limits currently imposed are likely to be contrary to the provision providing access to personal data in the data protection law. The relevant RBI Circular and CIC Rules will need to be modified so that they can be reconciled with the data protection law.

Part III of the White Paper (Grounds of Processing, Obligation on Entities and Individual Rights)

Chapter 1: Consent

1. What are your views on relying on consent as a primary ground for processing personal data?

Alternatives:

a. Consent will be the primary ground for processing.
b. Consent will be treated at par with other grounds for processing.
c. Consent may not be a ground for processing.

We believe that take consent prior to data collection should continue to be an important part of a future data protection regime. However, consent should not be the primary ground for processing. We propose a test of legitimate purpose should be the primary grounds for collection and processing of personal data. This is described in detail in our response to the questions in section 4.5, Part III of the White Paper.

The shortcomings of the notice-and-consent model when it comes to protecting individuals' interests are well known, and also described in the White Paper. Research has also shown that several behavioural biases and cognitive limitations operate on individuals' decision-making about personal data (Solove, 2012; Merz and Fischhoff, 2009; Acquisti and Grossklags, 2015). In the Indian context, our recently concluded qualitative study (cited on page 79 of the White Paper) revealed that people are often not aware that their personal data is stored or shared by service providers, despite accepting terms and conditions through which their consent is ostensibly collected (CGAP, Dalberg and Dvara Research, 2017). Especially in a country like ours, where many Indians are using data-driven services for the first time and yet to fully understand to better self-manage their privacy, it would be unwise to rely on consent as the sole grounds for processing.

However, setting out prescriptive rules on how data can be used would be untenable in this context, given the constantly changing nature of services and of technology. Such an approach could also interfere with individuals' choice and freedom to share their data where they stand to gain benefits or services. This autonomy with regard to decision making is considered a part of privacy, and the use of consent as a basis for sharing and processing of personal data is underpinned by this principle of decisional autonomy (Acharya, 2015).

Accordingly, we believe that consent should remain an important aspect of a future data protection law. However, the role of consent has changed. It must act to empower individuals and the regulator by putting them on notice regarding how their personal data will be used, with the option to opt out of the collection if required. However, consent must not be the basis for overriding obligations or protections mandated by the future data protection law (except in certain clearly defined situations, such as for medical emergencies). Entities must still make an assessment of legitimate purpose prior to collecting or using personal data, and this should be the primary test for processing obligations of entities using personal data, as further described in our responses to section 4.5, Part III of the White Paper.

2. What should be the conditions for valid consent? Should specific requirements such as 'unambiguous', 'freely given' etc. as in the EU GDPR be imposed? Would mandating such requirements be excessively onerous?

In our view, "consent" means the specific, informed and unambiguous acceptance by an individual, who is not under any duress or undue influence of any entity or third party at the time of such acceptance, through clear, affirmative action signifying agreement of the individual to the collection of personal data relating to him or her. For children, consent should be received from a person with parental responsibility for the child whose personal data is being sought to be collected.

In particular, we propose that entities should apply the legitimate purpose test (as described in our response to section 4.5, Part III of the White Paper) prior to collection of personal data. This means consent should only be requested for personal data that the entity has a legitimate purpose to access. Where entities seek to use any personal data previously collected for a different purpose, they should go back to the individual to request consent for these new uses. We do not think that this will result in individuals being inundated with requests for consent. On the contrary, if the entity collecting data applies the legitimate purpose test and has a well-designed just-in-time consent requests in place it would result in the individual being asked for consent only in particular circumstances in a meaningful manner.

Further, as noted in response to question 4 below of this section, consent should be requested in close proximity to time and location of the collection of the personal data, in a clear, and conspicuous and prominent manner. The entity requesting consent should also consider the context for which it is being obtained, and use clear and plain language taking into account the level of understanding and communications skills of the individuals whose consent is likely to be sought.

3. How can consent fatigue and multiplicity of notices be avoided? Are there any legal or technology-driven solutions to this?

The White Paper correctly recognises the fatigue that is associated with the variety of privacy notices and consent agreements that are placed before individuals. We believe there are two steps by which consent fatigue can be reduced.

First, entities should apply the legitimate purpose test (as described in our response to section 4.5, Part III of the White Paper) prior to collection of personal data. This should reduce the number of times that consent is requested for personal data that the entity has a legitimate purpose to access.

Second, such fatigue can be reduced with improvements in the design of such notices and the implementation of how consent is obtained (ENISA, 2014). An important opportunity exists for the India to incentivise the development well-designed, layered and contextual notices that ask for consent "just-in-time" in a manner that makes it easy for users to understand the salient points being highlighted in such notifications (Schaub et al, 2015).

The market at large should be allowed to improve how consent for data processing is obtained within the broad regulations mandated by the data protection law. To aid in this development, which may use a variety of legal or technology driven solutions, the regulatory authority should continuously evaluate and compare the different methods of operationalising consent.

4. Should different standards for consent be set out in law? Or should data controllers be allowed to make context-specific determinations?

In our model, any entity collecting personal data would apply the test of legitimate purpose prior to collection to make a contextual determination of whether such collection is required. Given this contextual determination is being made by the entity, the law should set out clear requirements that notices and consent mechanisms should incorporate at a minimum.

5. Would having very stringent conditions for obtaining valid consent be detrimental to day-to-day business activities? How can this be avoided?

As mentioned in our response to question 2 of this chapter, in our view, the combination of a legitimate purpose and well-designed just-in-time consent request should significantly reduce the volume of consent requests that an entity needs to make. Once an entity implements such data use policies, in our view, subsequent impact on the day-to-day business activities of the entity is likely to be minimal. This should overall reduce the impact on the day to day activities. Such a process not only reduces the effects of consent fatigue on individuals but in the long term is likely to reduce the overall cost of compliance with data protection regulations.

6. Are there any other views regarding consent which have not been explored above?

Chapter 2: Child's Consent

1. What are your views regarding the protection of a child's personal data?

2. Should the data protection law have a provision specifically tailored towards protecting children's personal data?

3. Should the law prescribe a certain age-bar, above which a child is considered to be capable of providing valid consent? If so, what would the cut-off age be?

4. Should the data protection law follow the South African approach and prohibit the processing of any personal data relating to a child, as long as she is below the age of 18, subject to narrow exceptions?

5. Should the data protection law follow the Australian approach, and the data controller be given the responsibility to determine whether the individual has the capacity to provide consent, on a case by case basis? Would this requirement be too onerous on the data controller? Would relying on the data controller to make this judgment sufficiently protect the child from the harm that could come from improper processing?

6. If a subjective test is used in determining whether a child is capable of providing valid consent, who would be responsible for conducting this test?

Alternatives:
a. The data protection authority
b. The entity which collects the information
c. This can be obviated by seeking parental consent

7. How can the requirement for parental consent be operationalised in practice? What are the safeguards which would be required?

8. Would a purpose-based restriction on the collection of personal data of a child be effective? For example, forbidding the collection of children's data for marketing, advertising and tracking purposes?

9. Should general websites, i.e. those that are not directed towards providing services to a child, be exempt from having additional safeguards protecting the collection, use and disclosure of children's data? What is the criteria for determining whether a website is intended for children or a general website?

10. Should data controllers have a higher onus of responsibility to demonstrate that they have obtained appropriate consent with respect to a child who is using their services? How will they have — actual knowledge of such use?

11. Are there any alternative views on the manner in which the personal data of children may be protected at the time of processing?

Chapter 3: Notice

1. Should the law rely on the notice and choice mechanism for operationalising consent?

We agree with the Committee's view that notice is important as it operationalises consent. The future law must contain requirements on the form and substance of the notice that must be delivered by entities prior to collecting personal data from individuals. However, we also reiterate our position that although notice and consent should remain an aspect of a future data protection law, it cannot be the basis for overriding obligations imposed on entities collecting data under the law. Entities should instead use an assessment of legitimate purpose prior to collecting or using personal data, pursuant to a legal test as set out in our responses to section 4.5, Part III of the White Paper.

The future law must support the development of notices that are well-designed, contextual and made to an individual at a time that is proximate to the collection of their personal data.

2. How can notices be made more comprehensible to individuals? Should government data controllers be obliged to post notices as to the manner in which they process personal data?

A variety of methods can be used to make notices comprehensible to individuals. For instance, the use simple language instead of 'legalese' in notices, allowing them to "show" rather than "tell" i.e. instead of simply describing practices a notice could describe the results that a particular practice is expected to achieve (Calo, 2012) . An important parallel from the financial sector is the development of the "Schumer Box" which discloses the terms and conditions of credit card agreements to help consumers easily get a snapshot of the salient points of the agreement they are entering into (DiGangi, 2017). Our recent study "Privacy on the Line" also considered some early design principles that would be important in the Indian context when designing such notices (CGAP, Dalberg & Dvara Research, 2017). Other researchers have pointed out requirements and best practices for notice design by including relevant and actionable information in notices that are layered and contextualised, supported by technology which provides new opportunities to develop a better user interface (Schaub et al, 2015).

We propose that the future Indian data protection law should mandate that notice must be conspicuous, concise, timely, updated, transparent, intelligible and easily accessible form written in clear, plain and understandable language both in English and predominant language of the individual's geographical area (if it is determinable). Where a significant portion of the target population is likely to have limited literacy skills, entities should be encouraged to give notice using appropriate visual and written formats. The future Data Protection Authority would be free to give more granular guidance on the format and substance of notices.

Further, we also propose that the law should mandate that entities collecting data should provide privacy notice comprising the following information:

(i) name and contact information of the data controller or its representative
(ii) voluntary or mandatory nature of data collection and associated consequences
(iii) contact for revoking consent
(iv) purpose for which data is being collected
(v) details of personal data collected from third parties
(vi) information related to whom the data may be disclosed to\
(vii) description of right to access/withdraw shared personal data
(viii) information regarding any form of automated data processing that may be carried out.

3. Should the effectiveness of notice be evaluated by incorporating mechanisms such as privacy impact assessments into the law?

4. Should the data protection law contain prescriptive provisions as to what information a privacy notice must contain and what it should look like?

Alternatives:
a. No form based requirement pertaining to a privacy notice should be prescribed by law.
b. Form based requirements may be prescribed by sectoral regulators or by the data protection authority in consultation with sectoral regulators.

We do believe that a future data protection law would benefit from setting out certain basic elements that all notices should contain across all sectors or industries. The data protection authority could provide further guidance with regard to the contents of a notice by publishing appropriate guidelines/regulations, in collaboration with sectoral regulators.

Some of the minimum requirements for any notice to comply with the data protection law should include, (i) name and contact information of the data controller or its representative, (ii) voluntary or mandatory nature of data collection and associated consequences, (iii) contact for revoking consent, (iv) purpose for which data is being collected, (v) details of personal data collected from third parties, (vi) information related to whom the data may be disclosed to, (vii) description of right to access/withdraw shared personal data and (viii) information regarding any form of automated data processing that may be carried out.

5. How can data controllers be incentivised to develop effective notices?

Alternatives:
a. Assigning a 'data trust score'.
b. Providing limited safe harbour from enforcement if certain conditions are met.

If a 'data trust score' is assigned, then who should be the body responsible for providing the score?

6. Would a consent dashboard be a feasible solution in order to allow individuals to easily gauge which data controllers have obtained their consent and where their personal data resides? Who would regulate the consent dashboard? Would it be maintained by a third party, or by a government entity?

7. Are there any other alternatives for making notice more effective, other than the ones considered above?

Chapter 4: Other Grounds for Processing

1. What are your views on including other grounds under which processing may be done?

We agree with the views of the Committee that in the modern context, consent cannot be the sole grounds under which processing of data may be carried out. We propose a test of legitimate purpose should be the primary grounds for collection and processing of personal data.

The White Paper briefly considers other grounds of processing including "legitimate interest" on page 100, before noting that they would require modification and further examination to be applied in India. We have undertaken this examination of various potential tests that can be applied for data protection, especially given the obvious failings of the notice-and-consent model. Our analysis leads us to believe that a simple and elegant "legitimate purpose" test (as set out below) would be an important step forward in India that would avoid reinventing the broken wheel of existing models. This formulation draws from the of Moerel and Prins (2016) among other thinkers, and the analysis around the concept of "legitimate interest" in the EU GDPR. However, we propose that a simpler and more elegant formulation for use in India, relying squarely on whether the use of personal data is

(i) lawful i.e. not illegal;
(ii) necessary i.e. required by the relevant entity to perform the service in question; and
(iii) proportionate i.e. that the interests of the relevant entity does not override the interests of an individual as provided for under the law.

In order to be helpful to the Committee, we would like to humbly submit the following potential drafting language for such a test in the Indian context.

> *""legitimate purpose" means, with respect to personal data of an individual, the* ***legal, fair, necessary, proportionate and transparent*** *use, disclosure and retention of personal data which is:*
>
> *i. limited to what is necessary for performance of a service or provision of a product or at a stage immediately prior to performing the service or providing a product , and where no less intrusive means are available; or*
> *ii. required in furtherance of a legal obligation; or*
> *iii. necessary for administration of justice pursuant to a court order; or*
> *iv. required for performance of any statutory, governmental or other functions by data processor or data controller as duly specified to the individual subject to data collection; or*

v. *necessary to protect the vital interests of the individual or of another individual, particularly where the individual is a child, including but not limited to the case of an individual's medical emergency which is fatal or may likely lead to permanent or irreversible bodily harm; or*

vi. *necessary for the third party to whom data is disclosed after it is duly informed to the individual, provided that the interests of data processors or data controller or third parties shall be adequately balanced against any prejudicial effect of the same on the rights and freedoms of the individual as guaranteed under this Act:*
***Provided that** the interests of data processors or data controllers or third parties does not override the interests, rights and freedoms of the individual as provided under the Constitution of India;"*

This test would need to be applied by entities collecting and processing data throughout the data life cycle i.e. prior to collecting personal data, before processing it, and to assess whether the personal data can be retained, disclosed or shared. If the test is not passed, the relevant activity should not be undertaken. In our view, a legitimate purpose test allows for a wider cost-benefit analysis which considers not only implications and privacy risks for individuals and society as well as potential benefits which the processing of data may result in for both the individuals as well as society as whole. Read with our approach to enforcement and supervision as set out in our responses to Part IV of the White Paper, we believe this formulation provides a compelling alternative to the notice-and-consent model.

Entities using personal data to provide goods and services are most well placed to make this determination, especially as they are rooted in the context and at the coal-face of data use. More granular secondary regulation together with industry codes of practices could be used to flesh out what constitutes "legitimate purpose" in particular industry contexts, working with sectoral regulators where appropriate.

2. What grounds of processing are necessary other than consent?

As noted in our response to question 1 of this section 4.5 and the questions in section 1.5, Part III of the White Paper, consent should no longer be the primary grounds for the processing of personal data. We propose that the "legitimate purpose" test as set out above should be used to determine whether a particular use of personal data was valid or in contravention of the data protection law. This test would need to be applied by entities collecting and processing data throughout the data life cycle i.e. prior to collecting personal data, before processing it, and to assess whether the personal data can be retained, disclosed or shared. If the test is not passed, the relevant activity should not be undertaken.

3. Should the data protection authority determine residuary grounds of collection and their lawfulness on a case-by-case basis? On what basis shall such determination take place?

Alternatives:

a. No residuary grounds need to be provided.
b. The data protection authority should lay down 'lawful purposes' by means of a notification.
c. On a case-by-case basis, applications may be made to the data protection authority for determining lawfulness.
d. Determination of lawfulness may be done by the data controller subject to certain safeguards in the law.

As noted in our response to question 2 of this section, the proposed 'legitimate purpose' test includes all purposes which may be required as a ground for processing of data. Thus, in our view, there is no requirement for any other residuary grounds to be provided in the law.

4. Are there any alternative methods to be considered with respect to processing personal data without relying on consent?

Chapter 5: Purpose Specification and Use Limitation

1. What are your views on the relevance of purpose specification and use limitation principles?

We propose to the Committee that the principles that underlie purpose specification and use limitation are better considered within the framework of the legitimate purpose test that is set out in our responses to the questions in section 4.5, Part III of the White Paper. Given the context of modern technologies being adopted in the world of data processing which very often do not have a specific pre-determined purpose or use for the processing of data, it is important for these principles to be part of the contextual determination made by providers.

2. How can the purpose specification and use limitation principles be modified to accommodate the advent of new technologies?

As mentioned in the response to the previous question, these principles when applied within an overall legitimate purpose test rather than independently accommodate the advent of newer technologies.

3. What is the test to determine whether a subsequent use of data is reasonably related to/ compatible with the initial purpose? Who is to make such determination?

As outlined in our response to question 1 in this section, we are not in favour of the use limitation principle and the associated test of compatibility with the purpose as a ground for data processing.

4. What should the role of sectoral regulators be in the process of explicating standards for compliance with the law in relation to purpose specification and use limitation?

Alternatives:

a. The sectoral regulators may not be given any role and standards may be determined by the data protection authority.

b. Additional/ higher standards may be prescribed by sectoral regulators over and above baseline standards prescribed by such authority.

c. No baseline standards will be prescribed by the authority; the determination of standards is to be left to sectoral regulators.

We direct the attention of the Committee to our responses to the questions raised in Part IV of the White Paper. It is important that a future Data Protection Authority flesh out the contours of how the primary law will apply in specific contexts, and work with sectoral regulators to create this clarity where these exist in India.

As mentioned in our response to question 1 of this section, specifically with respect to the principles of purpose specification and use limitation, we think these should be applied within a broader test of legitimate purpose as described in our responses to Chapter 4 of this part of the White Paper. As mentioned, we believe that sectoral regulators, considering their better understanding of data processing within the respective sectors, will play an important role in the application of the legitimate purpose test by way of providing appropriate guidance to the entities which process data by way of regulations, informal guidelines or even responding to specific queries of data controllers.

5. Are there any other considerations with respect to purpose specification and use limitation principles which have not been explored above?

Chapter 6: Processing of sensitive personal data

1. What are your views on how the processing of sensitive personal data should be done?

As referred to in our responses to Part II of this White Paper, we do not think that a classification of data into "sensitive personal data" and "personal data" is not suited given the rapid changes in how personal data is generated and used, and especially in the context of modern data processing methodologies. The future law should apply to all personally identifiable data. With respect to the processing of such personally identified data, we believe that the use of a legitimate purpose test (as described in our response to Part III, Chapter 4 of the White Paper) allows for a more contextual assessment of whether the processing of data is appropriate in a given context. The test will allow the weighing potential harms associated with the processing of any data that may be considered 'sensitive' in nature as well as the potential benefits that may be derived from the processing of data for both at the level of an individual as well as the society as a whole.

2. Given that countries within the EU have chosen specific categories of ―sensitive personal data‖, keeping in mind their unique socio-economic requirements, what categories of information should be included in India's data protection law in this category?

As referred to in our responses to Part II of this White Paper, we do not think that a classification of data into "sensitive personal data" and "personal data" is not suited given the rapid changes in how personal data is generated and used, and especially in the context of modern data processing methodologies. The future law should apply to all personally identifiable data. Such an approach will also incentivise the development of de-identification techniques into the future.

3. What additional safeguards should exist to prevent unlawful processing of sensitive personal data?

Alternatives:
a. Processing should be prohibited subject to narrow exceptions.
b. Processing should be permitted on grounds which are narrower than grounds for processing all personal data.
c. No general safeguards need to be prescribed. Such safeguards may be incorporated depending on context of collection, use and disclosure and possible harms that might ensue.
d. No specific safeguards need to be prescribed but more stringent punishments can be provided for in case of harm caused by processing of sensitive personal information.

4. Should there be a provision within the law to have sector specific protections for sensitive data, such as a set of rules for handling health and medical information, another for handling financial information and so on to allow contextual determination of sensitivity?

5. Are there any alternative views on this which have not been discussed above?

Chapter 7: Storage Limitation and Data Quality

1. What are your views on the principles of storage limitation and data quality?

We agree with the provisional views of the Committee on the principles of storage limitation and recognise the difficulties associated with prescribing specific time limits for how long personal data should be retained. In our view, the legitimate purpose test we propose, as described in our response to Part III Chapter 4 of this White Paper, should also be applied to the retention of data.

This means that entities can make contextual decision on whether data can be retained, and if so how long personal data such retention can be carried on. Such an approach will also incentivise the development and use of de-identification techniques, where entities want to retain data to develop training data sets for innovation.

We also agree with the committee with regard to the importance of data quality, i.e. ensuring that personal data held by any entity should be accurate. In our view, the primary responsibility of ensuring accuracy should lie with the entity which has collected and is processing the data. In today's age, personal data of a single individual is held in a variety of forms across a large number of entities. In many cases, an individual may not even be aware of all entities which have access to her/his personal data. Thus, it is nearly impossible for the individual to track all her/his personal data and ensure that it is accurate. Nonetheless, the individual should continue to have the right to have her/his personal data corrected.

2. On whom should the primary onus of ensuring accuracy of data lie especially when consent is the basis of collection?

Alternatives:
a. The individual
b. The entity collecting the data

As outlined in our response to question 1 of this section, the entity collecting the data should have the primary onus of ensuring the accuracy of the data. We also call for a right to be given to all individuals to have his or her personal data updated, corrected or deleted by the entity, by making an application to that entity to make any required correction to ensure accuracy.

3. How long should an organisation be permitted to store personal data? What happens upon completion of such time period?

Alternatives:
a. Data should be completely erased
b. Data may be retained in anonymised form

The specific period for which an organisation is allowed to store personal data should be considered in context of the particular data processing as a whole. As mentioned in our response to question 1 of this section, the legitimate purpose test should be used to determine whether personal data needs to be retained. Once such data no longer needs to be retained, the data may either be completely erased or anonymised for further use. It must be noted, that entities using such anonymised data should ensure that the continues to remain anonymous in nature throughout its lifecycle.

4. If there are alternatives to a one-size-fits-all model of regulation (same rules applying to all types of entities and data being collected by them) what might those alternatives be?

5. Are there any other views relating to the concepts of storage limitation and data quality which have not been considered above?

Chapter 8: Individual Participation Rights-1

1. What are your views in relation to the above?

We strongly support the need to have a cluster of rights which guarantee the individual the ability to participate in the processing of their personal data.

However, we are at variance with the White Paper's formulation of this principle. We believe it is preferable for the individual to have two separate rights: a right that allows them access to their own personal data and a right to be put on notice about how their personal data will be processed. In the current articulation of the Provisional Views in this part, there is ambiguity around distinction between a right to notice about data processing and a right to access personal data.

A right to access personal data can work well only when the individual has sufficient information about the entities who are processing their data. In the absence of such information, the individuals are left to guess the entities that could have their personal data and then approaching them to gain access to their personal data that is being processed. This poses a daunting burden on the individuals, especially when not all individuals have the agency and wherewithal to pursue data processors. A right to access personal data without apriori information on who is processing the data can significantly reduce the effectiveness of the individual participation rights.

Individuals' right to be informed of the processing of their personal data is well served providing them a 'notice' at the time of collection. The notice should be conspicuous, concise, timely, updated, transparent, intelligible and provided in an easily accessible form written or depicted in the manner that is sensitive to the users' language preferences and literacy levels. We provide detailed inputs regarding the format and content of Notice in Chapter 3 of Part III.

We propose the following, twin formulation for a distinct right to access personal data:

(1) Every individual shall have access to personal data from such individual or generated by or associated with that individual's personal data, which is collected, processed, used or stored by an entity, and such access will be provided:

(a) Upon proper identification;
(b) within a reasonable time not to exceed ten business days;
(c) at no charge or a nominal charge;

(d) in a reasonable manner, and through a clear user interface that allows them to make informed choices about who sees their data, how it is used, and where and how it is stored;
(e) where possible, through the same medium in which the information was provided; and
(f) in a form that that can be retained and is intelligible to the individual.

(2) When access to personal data is provided, the individual shall be informed of:

(a) The purposes of processing the information;
(b) the recipients of such information;
(c) whether the individual's national identifier is provided;
(d) the period for which such information will be retained;
(e) the right to dispute such information and request that it be corrected or erased;
(f) the right to lodge a complaint with the Authority;
(g) where the information was not collected from the individual, information about the source of the information;
(h) the existence of automated decision making and profiling.

We believe that the above formulation in conjunction with a right to be informed about data processing will make for meaningful individual participation in data processing.

2. Should there be a restriction on the categories of information that an individual should be entitled to when exercising their right to access?

The individual should have the right to access personal data that an entity has collected directly from the individual as well as any personal data that is generated or associated with the individual's personal data.

To reiterate, personal data refers to any information that related to an individual which, either directly or indirectly, including in combination with other information available or likely to be available is, capable of identifying such individual. The identifiability of information is a crucial barometer for the application of data protection laws and principles. Information that has been de-identified or is non-identifiable is not required to be shared with the individual.

The exercising of this right by an individual should not contravene with the rights of other individuals.

3. What should be the scope of the right to rectification? Should it only extend to having inaccurate date rectified or should it include the right to move court to get an order to rectify, block, erase or destroy inaccurate data as is the case with the UK?

If an individual believes that his or her personal data is inaccurate, untimely, incomplete or unlawfully collected he or she should have the right to get it corrected, updated or deleted by the processing organisation.

Similar to the provisions of jurisdictions like South Africa (Section 24(1)(a) of the Protection of Personal Information (PoPI) Act, 2013), the entities that possess the contested personal data should be the first point of remedy. The individual should have a mechanism to challenge the data being processed by the entity, by the way of making an application.

Post the individual's application, the organisation should be given reasonable time, we propose, thirty calendar days to examine the individual's challenge and take necessary steps to correct, update or delete the data, accordingly. Any changes arising in personal data should be systematically communicated to third parties that were provided access to the data.

To prevent any harm due to inaccuracy of data, the entity should restrict the processing of disputed data, while the claims of individuals are still under examination. Though it is the individuals' responsibility to have their data corrected, at their end, the entities should also take reasonable steps to ensure the timeliness, correctness and completeness of personal data that they process.

4. Should there be a fee imposed on exercising the right to access and rectify one's personal data?

Alternatives:
a. There should be no fee imposed.
b. The data controller should be allowed to impose a reasonable fee.
c. The data protection authority/sectoral regulators may prescribe a reasonable fee.

5. Should there be a fixed time period within which organisations must respond to such requests? If so, what should these be?

Yes, requiring the data controllers and processors to respond to challenges to the accuracy, timeliness and legality of personal data will ensure that incorrect or unlawful data is not used indefinitely to make significant decisions about individuals.

An organisation should be granted reasonable time to verify the claims of the data subject and respond accordingly. We propose that entities should be allowed a response time of thirty calendar days at the expiry of which the consumer should have the right to file a complaint with the proposed data protection authority.

6. Is guaranteeing a right to access the logic behind automated decisions technically feasible? How should India approach this issue given the challenges associated with it?

7. What should be the exceptions to individual participation rights? [For instance, in the UK, a right to access can be refused if compliance with such a request will be impossible or involve a disproportionate effort. In case of South Africa and Australia, the exceptions vary depending on whether the organisation is a private body or a public body.]

8. Are there any other views on this, which have not been considered above?

Chapter 9: Individual Participation Rights-2

1. What are your views in relation on the above individual participation rights?

We agree with the White Paper's position on empowering the individual with the rights to participate in the processing of their personal data. The right to be informed about such processing and the right to seek their personal data in a machine-readable format go a long way in empowering the individual.

However, we believe that the individual should have the right to withdraw consent and have their personal data returned and deleted by the entity. Revoking consent should be as easy as providing it.

2. The EU GDPR introduces the right to restrict processing and the right to data portability. If India were to adopt these rights, what should be their scope?

As emphasised above, the individuals should have the right to revoke consent to the processing of their personal data.

Moreover, the individuals should have the right to portability of their personal data. The individuals should be entitled to transmit their personal data from the data controller who was the original collector or generator of the personal data, to another specified data controller without

hindrance. Moreover, the individuals should have the right to have the personal data transmitted directly from one entity to the other wherever it is technically feasible and possible.

These provisions will allow for a secure and robust flow of data that is needed for the growth of the digital economy.

3. Should there be a prohibition on evaluative decisions taken on the basis of automated decisions?

Alternatives:
a. There should be a right to object to automated decisions as is the case with the UK.
b. There should a prohibition on evaluative decisions based on automated decision making.

Automated and algorithmic decision making can have significant implications for individuals. They can impact the ability and price at which they avail of financial products like credit, insurance and non-financial products and services. (Comandé, 2017)

In order to contain the likelihood of adversarial effects of data we propose that the data controller or processor using automated tools should, through a prior demonstration show that the automated tool is predictive for a legitimate purpose and is non-discriminatory with respect to the protected characteristics recognised in the Constitution of India. Moreover, algorithms could also be subjected to audits by the proposed data protection authority to understand their working.

The data controllers or processors using algorithms should provide the meaningful information on the logic of the algorithm as well as the envisaged consequences of such processing for the individuals.

4. Given the concerns related to automated decision making, including the feasibility of the right envisioned under the EU GDPR, how should India approach this issue in the law?

Please refer to answer 3, above.

5. Should direct marketing be a discrete privacy principle, or should it be addressed via sector specific regulations?

6. Are there any alternative views in relation to the above which have not been considered?

Chapter 10: Individual Participation Rights-3: Right to be forgotten

1. What are your views on the right to be forgotten having a place in India‘s data protection law?

2. Should the right to be forgotten be restricted to personal data that individuals have given out themselves?

3. Does a right to be forgotten add any additional protection to data subjects not already available in other individual participation rights?

4. Does a right to be forgotten entail prohibition on display/dissemination or the erasure of the information from the controller‘s possession?

5. Whether a case-to-case balancing of the data subject‘s rights with controller and public interests is a necessary approach for this right? Who should perform this balancing exercise? If the burden of balancing rests on the data controller as it does in the EU, is it fair to also impose large penalties if the said decision is deemed incorrect by a data protection authority or courts?

6. Whether special exemptions (such as the right to freedom of expression and information) are needed for this right? (over and above possible general exemptions such as national security, research purposes and journalistic or artistic expression)?

7. Are there any alternative views to this.

Part IV of the White Paper (Regulation and Enforcement)

Chapter 1: Enforcement Models

1. What are your views on the above described models of enforcement?

While the three paradigms described by the Committee are useful to frame the discussion on regulatory models, we would like to also bring the Committee's attention to an important regulatory framework that has not been considered in the White Paper. This relates to **responsive regulation**, a well-developed academic theory[14] and a widely accepted regulatory framework[15], which is a dynamic, context-sensitive framework that incorporates multiple kinds of sanctions from all categories of regulation recognised in the White Paper (Greenleaf, 2014). By collapsing the regulatory spectrum into three unnecessarily exclusive categories of 'command and control', 'self-regulation' and 'co-regulation', unfortunately it appears that the White Paper forces an unnecessary and inefficient choice between the various elements of each of these categories of regulation.

We think that data protection regulation will benefit from responsive regulatory framework which uses tools across the full spectrum of regulatory tools.

The crux of responsive regulation is a hierarchy of regulatory sanctions, through which the regulator can escalate. To begin with, the regulatory posture is collaborative and uses co-regulatory tools that include but are not limited to industry-proposed codes of conduct. The full spectrum of co-regulatory tools (in addition to codes of conduct, which are an important tool in themselves) should be considered for a future data protection framework. If there is a failure of co-regulation to satisfy the objectives of the regulator or a continuing violation of legal obligations, an escalated regulatory response can be used under a responsive data regulation framework. The magnitude of escalation and the punitive effect of the regulatory response will depend on the nature of default. The regulator's choice of the kind of sanction will be dependent on context, the nature of the default and the past behaviour of the faulting regulated entity, among other factors.[16]

The crux of responsive regulation is well illustrated through Ayer's and Braithwaite's widely recognised regulatory pyramid:

[14] Theory of Responsive Regulation was first proposed by Ayres and Braithwaite in their seminal book; Ayres, I., & Braithwaite, J. (1992). *Responsive Regulation: Transcenidng the Deregulation Debate.* New York, New York, USA: Oxford University Press.
[15] Ivec and Braithwaite take stock of the performance of responsive regulation across numerous sectors in Australia and other jurisdictions. For a complete discussion, see Ivec, M., & Braithwaite, V. (2015). *Applications of responsive regulation in Australia and overseas: update.* Regulatroy Institutions Network. Australia: Regulatory Instituions Network.
[16] Braithwaite, J. (2011). The Essence of Responsive Regulation. U.B.C. Law Review, 475-520.

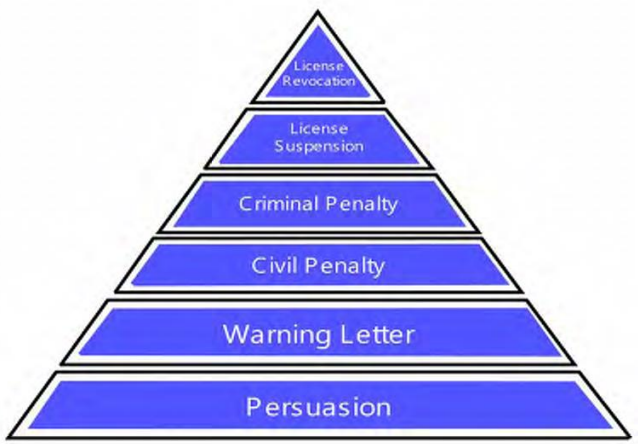

Figure 1: A typical regulatory pyramid.

Source: Application of responsive regulatory theory in Australia and overseas: update (p 66, Ivec & Braithwaite, 2015)

As seen from this pyramid, regulatory tools at the top of the pyramid are affiliated to the 'command and control' variant of regulation. Their placement at the top suggests that these tools correspond to the highest levels of regulatory escalation. The underlying game theoretic tenet of the model is that a credible threat of an ultimate, serious and costly regulatory imposition will encourage regulated entities to early on comply with the softer, cheaper regulations like persuasion, co-regulation and self-regulation. Compliance is incentivised by the threat of expensive and prohibitive regulatory sanctions.

The hierarchy of instruments should not be confused for the inability to use the more punitive regulatory sanctions. At no time, is the use of any of the regulatory responses excluded from the regulatory toolkit. Responsive regulation affords the flexibility and, context-sensitivity to the regulator that must be foregone when regulators are forced to choose between the two extremes of sanctions that are typical of command and control style of regulation and the industry-proposed, codes-of-conduct kind of co-regulation. Apart from being sensitive to context, responsive regulation is also appropriate to keep pace with constantly evolving technologies that continuously shape the realm of data protection continuously.

Neither data protection nor India is unfamiliar to the use of responsive regulation. The working of the American data protection regime closely corresponds to the responsive regulatory framework. The regulatory stance of the U.S Federal Trade Commission (FTC) closely resembles the increasing escalation illustrated in the regulatory pyramid. The FTC begins with the assumption of willingness of the regulated entity to comply with the law. Resolution for the first offence is often worked out privately between the FTC and the faulting company. The complaint and consent

decree are triggered simultaneously at the time of the first offence. As a consequence, the company is now subject to closer regulatory scrutiny through external audits and internal compliance programs. The FTC also gets greater powers of investigating the company post the first offence. This is an escalation along the responsive pyramid. Once a company is under the consent decree, subsequent offences are often treated as violations of the consent decree that empower the FTC to impose very heavy monetary penalties. These fines can be as high as USD 16,000 per individual violation that can be multiplied by the number of users and can be levied on a daily basis for continuing violations (McGeveran, 2016).

Similarly, the toolkit of existing Indian regulators like the Securities and Exchange Board of India (SEBI) have some elements of the gradual regulatory escalation found in the responsive regulation theory. Through the SEBI (SRO) Regulations 2004, SEBI has allowed for creation of and regulation through self-regulatory organisations. SEBI also offers informal guidance to companies directly and also issues direct orders while retaining powers for more punitive regulatory measures like investigating and penalising faulting companies[17].

The range of regulatory tools afforded by responsive regulation, allows for effective data protection by enabling the regulator [to] 'act, variously, as ombudsmen, auditors, consultants, educators, negotiators, policy advisers, and enforcers.' (McGeveran, 2016). The regulators are not expected to allocate same weights and priorities to each of these roles. They are expected to determine the most relevant regulatory stance in each context and tools of responsive regulation can provide them efficient and appropriate instruments of which co-regulation is just one. Moreover, it is widely accepted that data protection needs vary widely across sectors. For instance, the time frame for which the data needs to be retained in the health sector will vary significantly from the needs of the financial sector. Responsive regulation also permits the sectoral regulators the flexibility to create specific and nuanced regulation suited to the needs of their respective sectors.

2. Does co-regulation seem an appropriate approach for a data protection enforcement mechanism in India?

Co-regulatory approaches allow industry to enjoy considerable flexibility in shaping self-regulatory guidelines, with Government setting the default requirements and retaining general oversight authority to approve and enforce these guidelines (Sinclair, 1997). We think that co-regulation must be part of a wider toolkit for regulators in the data protection space. However, co-regulation of the variety that relies exclusively or predominantly on adherence to self-proposed codes of conduct by the industry may not be the best suited model for data protection in the Indian context. This could risk susceptibility to particular interest groups or particular powerful stakeholders within the industry.

Another concern that the experience from other countries has raised with a purely co-regulatory approach, is that it can lead to a 'check-box' based compliance with a view to minimise regulatory burden (McGeveran, 2016). Codes of conduct are likely to be more successful when the regulated sector comprises few regulated entities and the interests of the regulated entities align with public interests. Realising that these conditions are

[17] Securities and Exchange Board of India Act of 1992 (as amended by the Finance Act in 2017)

sparsely met in the context of data protection in India, there may be a need to complement codes of conduct with other methods of co-regulation. For instance, emerging research is revealing that other co-regulatory tools like privacy covenanting are likely to be more effective than codes of conduct (Rubenstein, 2010). Privacy covenants are contractual agreements between the regulator and the regulated entity and negotiations typically happen in the presence of citizens' interest groups. The advantage of such covenants is that they take the form of performance goals and not technology mandates. This holds businesses accountable for the outcomes achieved while providing for flexibility with regards to the technology used. More importantly, covenants can be negotiated sectorally and when complemented by government baselines, they can be more effective in achieving end outcomes (Rubenstein, 2010).

Finally, we note that vocabulary of Indian institutions also differs significantly from institutional settings where cooperation has evolved organically into the administrative state. Financial sector regulators have been only recently experimenting with codes of conduct and the evidence on their success is not conclusive.[18] Co-regulatory tools including codes of conduct should form one part of the full menu of regulatory tools across the pyramid of sanctions (as outlined in our response to question 1 in section 1.4, Part IV of the White Paper) used by a future data protection regime.

3. What are the specific obligations/areas which may be envisaged under a data protection law in India for a (i) 'command and control' approach; (ii) self-regulation approach (if any); and (iii) co-regulation approach?

4. Are there any alternative views to this?

Chapter 2: Enforcement Tools and Mechanisms

1. What are your views on the use of the principle of accountability as stated above for data protection?

We welcome the Committee's view that the future data protection law should reflect the principle of accountability, in particular with regard to the responsibilities of entities handling personal data. The efficacy of these rights will be reliant on the existence of a well-designed liability framework backed by a range of regulatory tools that can implement the principle of accountability in the practice of data protection.

To do so, we believe that the future law must create a system of user data rights to fulfil its core objectives i.e. to empower people to use their information as they desire and to protect people from undesirable harms (Chugh & Raghavan, 2017). Such rights will require legally binding

[18] Reserve Bank of India, Self-Regulatory Organisations for NBFC-MFI, 26 November 2016, found at https://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=30052, last accessed on 16 January 2018, See also, Securities and Exchange Board of India (Self-Regulatory Organisations) Regulations, 2004, found at https://www.sebi.gov.in/sebi_data/commondocs/sroregu_h.html, last accessed on 16 January 2018

obligations to be placed on entities handling and processing personal data, to ensure that they give effect to these rights and act in a way that will not contravene them. For example, if the future law makes provision for individuals to have a right to access and view their personal data after it has been collected by any entity, the corollary obligation on the relevant entity will be to create a clear user interface that allows the user to do so. We have made detailed submissions to the Committee in our responses to [Chapter 8, 9 and 10 in Part III] of the White Paper on the rights that the future law should create.

To operationalise these rights and obligations, the law must contemplate a three-pronged liability framework, that:

(i) imposes statutory strict liability for the majority of the data protection obligations which will be clearly set out requirements relating to the basis on which data can be collected, processed, shared or retained;

(ii) requires entities to take reasonable efforts to ensure personal data is not used in ways that cause harm to individuals or breaches their informational privacy; and

(iii) potentially create criminal offences for intentional misuse or sharing of personal data.

The formulation above will require an extension of the well-established doctrine of strict liability to certain data protection obligations, together with the creation of a definition of harm and of informational privacy for the purposes of the proposed law.

Strict liability standard for entities' processing obligations

Strict liability is the legal standard under which a party who has caused a loss (or the "injurer") must pay damages to the victim or injured party whether or not he or she was negligent (Shavell, 1982). The evolution of the doctrine can be traced back to the case of Rylands v Fletcher[19] ("***Rylands***") which involved the building of a reservoir dam by one party. The breach of the reservoir resulted in flooding in the surrounding lands, and the neighbouring party's coal mine resulting in the pronouncement that

> *"the person who, for his own purpose, brings on his land and collects and keeps there anything likely to do mischief if it escapes, must keep it in at his peril; and of he does not do so is prima facie answerable for all the damage which is the natural consequence of its escape."*

This "no fault" standard allocates liability based on the riskiness of the activity, on the logic that the person who amasses a substance which is likely to cause damage when it escapes should bear responsibility. It is well suited for extension to data protection regulations, especially to those conduct obligations that are set out *ex-ante* and expected of entities when they handle personal data. This approach has resonance with the effective deterrence theory that the leading Law and Economics scholar and jurist, Guido Calabresi (1970) has also examined. In this view, the law

[19] (1868) LR 3 HL 330.

should look at reducing the costs of accidents, and liability must attach itself to the "cheapest cost provider" party that is well suited to make a cost-benefit analysis between accident costs and accident avoidance costs (Calabresi, 1970). The application of this standard will also aid the development of the insurance market for data protection, as insurers will have clear requirements to assess should they look to provide liability insurance. The development of a good liability insurance market would ensure that this allocation of risk can be effectively managed by entities who will bear the liability (See further our response to question 6 of this chapter).

The future law should therefore codify the strict liability for the majority of the data protection obligations which will be clearly set out requirements relating to the basis on which data can be collected, processed, shared or retained.

Reasonable efforts to avoid harm or breach of informational privacy

To develop the idea proposed in the Committee's provisional view, the future law should also impose some liability for the causation of harm to individuals as a consequence of the inappropriate use of their data by entities. A potential definition for harm that could be used to define the concept in a future law could be:

> *"harm" is actual or potential injury or loss to an individual, whether such injury or loss is economic or non-economic, quantifiable or non-quantifiable*

Such a definition would build upon existing notions of harm that are already being articulated by regulators in other parts of the world. For instance, the US Federal Deposit Insurance Corporation's manual on evaluating consumer harm and risk of harm (US Federal Deposit Insurance Corporation, 2017). The European Commission has considered the notion of "consumer detriment" (page 24, European Commission, 2017), as have Australian authorities (Consumer Affairs Victoria, 2006). These notions bear relevance in the context of data. Solove and Citron's (2017) recent writing on harm in the context of data breach extends these notions theoretically in the context of data regulation.

We also propose that a similar obligation should be placed on entities to make reasonable efforts to access or process personal data in line with the right to informational privacy of individuals in India. A potential definition for a statutory right to informational privacy that could be included in a future data protection law could be:

> *"All individuals shall have a right to informational privacy pursuant to which they shall have the right to prevent information about themselves from being disseminated and to control the extent of access by any entity to their personal data."*

Such a definition would build on the conceptualisation of informational privacy in the *K.S.Puttaswamy v. Union of India*[20] matter. In that matter, the judges also referred to work by Koops et. al (p.568, 2017) which contains a pithy conceptualisation informational privacy as typified by the "*interest in preventing information about one-self to be collected and in controlling information about one-self that others have legitimate access to.*"

Given that these formulations will involve post-facto determinations, applying a strict liability standard for their breach appears difficult. We therefore propose that until such time as clearer definitions or standards evolve for these concepts, whenever a harm is caused or informational privacy is breached by data controllers or data processors their liability would be subject to the determination of whether they made reasonable efforts to avoid causing harm or breaching informational privacy.

Joint and several liability

We propose that where multiple entities are involved in a situation where personal data is compromised, resulting in the contravention of the future data protection regime then all such entities should be held jointly and severally liable. This means each of the parties liable can be held liable together or separately.[21]

Finally, upon the determination of liability, the adjudicating authority in question may have the discretion choose to employ a mix of remedies and enforcement tools (as further discussed in our responses to the questions posed in sections 1.4 and 2.21 in Part IV of the White Paper). While doing so, the authority should take into account:

- the nature and seriousness of the contravention;
- consequences and impact of the contravention including the extent of, benefit or unfair advantage gained by the entity, the loss and harm caused or likely to be caused to individuals, and the repetitive or continuing nature of the activity of the entity.

In summary, we believe the principle of accountability as envisioned in the White Paper would be best implemented by a system of user data rights that operationalises the core objectives of the data protection law, backed by a well-designed liability framework based on the principles set out above.

[20] (2017) 10 SCC 641

[21] Black's Law Dictionary, 7th Edition, (1999), p.219 "*(Of liability, responsibility, etc.) apportionable either among two or more parties or to only one or a few select members of the group, at the adversary's discretion; together and in separation.*"

2. What are the organisational measures that should be adopted and implemented in order to demonstrate accountability? Who will determine the standards which such measures have to meet?

The law should set out the principles of conduct that are expected from entities at each stage of the data life cycle from collection, processing, sharing, retention and destruction.

The standards that fulfil these conduct requirements should be laid out through secondary regulations or by the recognition of certain existing standards for existing industries.

These standards should also take into account the level of risk that is associated with the data processing activity that an entity is undertaking. Specifically, as noted in our responses to the questions raised in section 2.17, Part IV of the White Paper, we propose that data controllers could potentially be categorised into (1) systemically important data entities, (2) normal risk entities, and (3) low risk entities by a future regulator.

The future Data Protection Authority, working with relevant sectoral authorities for specialised sectors like finance, should work to develop a methodology and framework for the assessment of the level of risk posed by an entity, using quantitative as well as qualitative indicators taking into account various factors relevant to the data economy. This would also clarify the gradation in the specific standards of conduct expected from each type of entity.

3. Should the lack of organisational measures be linked to liability for harm resulting from processing of personal data?

As noted in response to question 1 of this section 2.5 of the White Paper, when harm is caused in this context then the liability of the data controllers or data processors should be subject to the determination of whether they made reasonable efforts to avoid causing harm. The absence of organisational measures to avoid harm from the misuse of data could be seen in such a determination as a factor indicating an absence of reasonable efforts.

4. Should all data controllers who were involved in the processing that ultimately caused harm to the individual be accountable jointly and severally or should they be allowed mechanisms of indemnity and contractual affixation of liability inter se?

Yes. As noted in response to question 1 of this section 2.5 of the White Paper, where multiple entities are involved in a situation where personal data is compromised, resulting in the contravention of the future data protection regime then all such entities should be held jointly and severally liable.

Mechanisms between the parties *inter se* should be the subject of private contract between them, as each entity involved will be best placed to understand and negotiate based on the particular risks they face.

5. Should there be strict liability on the data controller, either generally, or in any specific categories of processing, when well-defined harms are caused as a result of data processing?

Yes. As noted in response to question 1 of this section 2.5 of the White Paper, the future law should therefore codify the strict liability for the majority of the data protection obligations which will have clearly set out requirements relating to the basis on which data can be collected, processed, shared or retained.

6. Should the data controllers be required by law to take out insurance policies to meet their liability on account of any processing which results in harm to data subjects? Should this be limited to certain data controllers or certain kinds of processing?

In our view, a legal provision in legislation mandating insurance policies to meet liabilities that arise from harm caused will be a case of over-regulation. This can be allowed to develop through market practice, and where industry codes exist for incorporation in them as they evolve and as agreed between participants. In fact, as work from Shavell (1983) indicates **it is not socially beneficial for the government to intervene in the operation of competitive liability insurance markets**. This is especially because the terms at which insurance policies are sold in a competitive setting to some extent appropriately substitute the incentives to comply with such liability (p. 121-122, Shavell, 1983).

The future data protection law should limit itself to clearly defining the liabilities of the various entities involved in processing of personal data and the associated penalties, and remedies. It should then allow the market to develop in response, including the insurance market in relation to these liabilities.

7. If the data protection law calls for accountability as a mechanism for protection of privacy, what would be impact on industry and other sectors?

It is unclear that the requirement to have better data practice would enforce prohibitive costs for industry, especially given that it is in the interest of organisations to secure their data and maintain its quality. Several entities are already likely to have internal processes to do so. As analysis by those like Shavell (1983) show, liability insurance mechanisms can also develop to smoothen the costs of the risk allocation mechanisms that the law will put in place.

In any event, it is undeniable that some accountability mechanism needs to be included in Indian law even if this may result in some up-front costs of compliance. However technological solutions could be used to reduce these costs of compliance.

8. Are there any other issues or concerns regarding accountability which have not been considered above?

Chapter 2A: Enforcement Tools and Mechanisms: Codes of Practice

1. What are your views on this?

Voluntary codes of conduct can be used in the future data protection framework, as one part of a responsive model which includes aspects of co-regulation. However, it is re-iterated that codes of conduct are only one of many co-regulatory tools and must be used alongside them to achieve holistic regulation. Active oversight for compliance to codes of conduct can impose significant costs on the regulator.

Apart from being expensive to oversee, a model of co-regulation designed on codes of conduct also suffers from the following:

- *Codes of Conduct may be inclined to address the concerns of the industry i.e. businesses over all stakeholders and public policy objectives:* The reservation against entirely industry-proposed voluntary codes of conduct is that they may over- represent the concerns of industry or particular stakeholders within industry. To protect against this, while calling for such codes of conduct, the regulator should strive to ensure representation of all stakeholders through the creation of a self-regulatory organisation. One possible mechanism of doing this is to call for creation of self-regulating organisations that voice concerns of all stakeholders. This is seen in the Reserve Bank of India's Self-Regulatory Organisations for NBFC-MFIs' Criteria for Recognition expressly states that the self-regulatory body should consider the concerns of all stakeholders and not act as an industry body only.

- *Voluntary codes of conduct may not carry legal weights and get reduced to 'best practices':* This has been seen in data protection regulation of other jurisdictions where industry codes of conduct are often treated as recommendations and not binding in nature. For instance, the Irish Data Protection Law rests on a model of co-regulation but there are few instances where the industry has been forthcoming with the rules and most self-regulation focuses on public entities (McGeveran, 2016). Even where industry does propose self-regulation, since they lack legal sanction they can often be treated at best as 'best practice'. A relevant recent example from the United States is the creation of Network Advertising Initiative (NIA) when the Federal Trade Commission signalled the need for regulation of online preference marketing industry—an industry that used the cyber footprint, cookies and web bugs for creating user profiles for targeted advertising. The NIA is an industry led self-regulation program based on voluntary code of conduct. It has been noted to suffer deficiencies like a lack of internal auditing and compliance check of members, a "free rider problem" where members feign compliance, and poor choices of technology to meet stated objectives leading to less than satisfactory outcomes (Rubinstein, 2010).

- *The success of codes of conduct hinges on a set of peculiar preconditions that are not necessarily characteristic of the data protection landscape or Indian institutional architecture:* Both academic research (Priest, 1997-98) and regulatory experience (Australian Communications and Media Authority, 2011) suggest that co-regulation based on codes of conduct is likely to be successful when there are relatively fewer players in the industry, competing intensely around relatively homogenous products. This certainly does not appear to be the case when considering the wide spectrum of actors, services and goods that are likely to be the subject of a future data protection regulation. Co-regulation may prove to be more effective when the incentives of industry align well with public policy objectives of the regulator. However, when the two diverge, co-regulation may need to be complemented with higher engagement with the regulator.

2. What are the subject matters for which codes of practice may be prepared?

Codes of conduct can be used to design the processes and manner in which providers seek to achieve the benchmark set out in the primary legislation.[22]

Codes of conduct should be seen as a tool to supplement the main legislation by designing cost efficient and effective mechanisms to achieve the objective of the legislation. Seen in this light, codes of conduct serve to flesh out and contextualise the principles embedded in the legislation. This is particularly important, since these principles will need to be adapted to different sectors of the economy. Especially in specialised sectors, such as medicine and finance, the creation of conduct is best left to the expertise of the sector-specific regulators. It is not uncommon for sector-specific regulators to have laws for data protection and security. The Reserve Bank of India issues directions for data security and protection practices of Prepaid Instruments[23] and Outsourcing Guidelines for Banks[24] as well as Cyber Security Frameworks[25] for banks. Similarly, Securities and Exchange Board of India (SEBI) incorporates data sharing clauses in various regulations based on the specific context like SEBI (Debenture Trustees) Regulations, 1993, SEBI (Bankers to an Issue) Regulations, 1994, SEBI (KYC (KRA) Registration Agency) Regulations, 2011. Similar specific, data sharing clauses can also be found in Insurance Regulatory and Development Authority of India (IRDAI) and the Pension Fund

[22] The Australian Privacy Act of 1988 recommends 13 Australian Privacy Principles (APP). Under Section III-B of the Privacy Act, any entity that attracts APP can develop a written code of practice for the handling of personal information, called an APP code. An APP code sets out how one or more of the APPs are to be applied or complied with, and the APP entities that are bound by the code. (Office of Australian Information Commissioner, 2013, found on https://www.oaic.gov.au/agencies-and-organisations/advisory-guidelines/guidelines-for-developing-codes#part-1-introduction, last accessed on January 16 2018). Thus while the principles are defined in the legislation and are not negotiable, codes of conduct are encouraged around how entities choose to apply them. This prevents dilution of the protection offered in the legislation.

[23] See for example Clauses 15.1, 16.4, 17.5 (vii) and (viii) in Reserve Bank of India's Master Directions on Issuance and Operation of Prepaid Payment Instruments in India, 20 March 2017, found on https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=3325, last accessed on 16 January 2018.

[24] See for example Claus 5.5.1 of the Outsourcing Agreement in Reserve Bank of India's Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks, 3 November 2006, found on https://www.rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=3148 , last accessed on 16 January 2018.

[25] Reserve Bank of India, Cyber Security Frameworks for Banks, 2016, found on https://www.rbi.org.in/scripts/BS_CircularIndexDisplay.aspx?Id=10435, last accessed on 24 January 2018.

Regulatory and Development Authority. For a detailed discussion, please refer to our response on Chapter 10: Allied Laws of Part I of this White Paper.

Therefore, in instances where the existing sectoral regulators are already closely scrutinising the conduct of regulated entities, utilising their regulatory infrastructure will prevent risk of regulatory arbitrage. Moreover, the sector-specific regulators are more aware of issues that have significant welfare implications and are better situated to determine what aspects of data protection should be exposed to higher regulatory action. This requires a deep sensitivity to sector-specific issues as well as regulatory flexibility and should be the subject matter of codes of conduct.

Where sectoral regulators do not exist, it is for the proposed data regulator to initiate creation of codes of conduct from organisations that are able to demonstrate their representativeness. One way in which the body can assure the regulator of its representativeness is by creating a robust mechanism for consultation with all stakeholders. The Office of the Australian Information Commissioner is particularly attentive to the consultation process that has been used to create a code of conduct. The Commissioner reserves the right to not register codes that it identifies as being inadequately representative. (Office of Australian Information Commissioner, 2013)

3. What is the process by which such codes of conduct or practice may be prepared? Specifically, which stakeholders should be mandatorily consulted for issuing such a code of practice?

Where sectoral regulators exist, they can be vested with the responsibility of creation of codes of conduct to the satisfaction of the data regulator. The data regulator can lay out the objectives and desirable outcomes of the codes of conduct and leave it to the sectoral regulator to design a mechanism for the creation of code of conduct. Sectoral regulators are likely to have self-regulating organisations or existing codes of conduct for their specific sectors which can be expanded to cover data practices. Sectoral regulators must aspire to become more consultative over time by exposing proposed regulations to wider scrutiny. One way in which this can be done is by inviting public consultations on draft regulations, allowing for appropriate response- times and making counter comments possible.

Where sectoral regulators do not exist, the Data Protection Authority could invite codes from associations or groups of entities operating in a particular sector. While it may not necessarily prescribe qualification criteria for the bodies that can submit codes of conduct, it is desirable for the proposed data regulator to judge the proposed code of conduct on the basis of the procedure used in its creation. It is desirable to have a code of conduct that is endorsed by many, diverse stakeholders. Regardless of the consultative process underlying the creation of the code, the data regulator must necessarily invite public consultation on the code and hold stakeholder meetings to understand the response of the ecosystem.

The data regulator can be informed of the compliance to these codes of conduct through inter-sectoral coordination and information sharing. An effective mechanism way to achieve inter sectoral coordination is through the signing of Memorandum of Understanding (MoU).[26] In all cases, the codes of conduct must be clearly and conspicuously laid out on the website of the data regulator. These codes must also be periodically reviewed and edited. The website must carry the most recent version at all times.

4. Who should issue such codes of conduct or practice?

Please see our response to question 5 posed in section 2.10 of Part IV of the White Paper.

5. How should such codes of conduct or practice be enforced?

The enforcement of the codes should be left to the body proposing the code. The proposing body can be mandated by law to submit compliance reports to the data regulator. In addition to self-reporting, the data regulator could also use tools like mystery shopping and surprise audits to ensure compliance with codes. It has been shown that codes of conduct are more likely to be effective where their adoption is not voluntary but mandated by the law (Rubinstein, 2010). When accepting codes of conduct the data regulator should be conscious of enforcement costs and where it finds the costs of compliance and enforcement very high for successful uptake of the code, it must guide the representative body to reduce them. Given the high cost of monitoring compliance, the data regulator must satisfy itself of the resources and capacity of the body that proposes the codes of conduct.

6. What should be the consequences for violation of a code of conduct or practice?

Please see our response to question 5 above posed in section 2.5 of Part IV of the White Paper.

7. Are there any alternative views?

[26] See the Draft Indian Financial Code on the use and content of the Memorandum of Understanding that can be used to achieve intersectoral cooperation and coordination. Found on http://www.prsindia.org/uploads/media/draft/Draft-%20Indian%20Financial%20Code,%202015.pdf, last accessed on 16 January 2018. More generally the Federal Trade Commission has signed Memorandums of Understanding with American and international regulators to protect consumers in the context of their personal data.

Chapter 2B: Enforcement Tools and Mechanisms: Personal Data Breach Notification

1. What are your views in relation to the above?

In our view, only those breaches that result in revealing particular categories of sensitive data (as set out below) and likely to cause harm should trigger a breach notification. This list of sensitive data types is provided so that entities can have clear stipulations in the primary data protection legislation as to the types of breaches for which immediate notification must be given. The categorisation is solely for this purpose and not to otherwise indicate that there should be a gradation in the manner in which any personal data is treated. The particular types of sensitive data of an individual which trigger breach notification would involve information relating to or which serves to reveal:

i. racial or ethnic origins, political or religious views;
ii. passwords;
iii. financial information such as bank account or credit card or debit card or other payment instrument details or financial transactions records or other information that would permit access to an account;
iv. physical, physiological and mental health condition;
v. sexual activity;
vi. medical records and history;
vii. biometric data relating to the physical, physiological or behavioural characteristics of a natural person which allow their unique identification including, but not limited to, facial images, genetic information, fingerprints, handprints, footprints, iris recognition, handwriting, typing dynamics, gait analysis and speech recognition;
viii. any details relating to clauses (i) to (vii) above as provided to body corporates for providing service; and
ix. any of the information received under clauses (i) to (vii) above by body corporates for processing, stored or processed under lawful contract or otherwise.

If a breach of such sensitive data occurs, the relevant entities must then assess if there is a risk that harm will be caused to individuals as a result. Harm would include actual or potential injury or loss, whether such injury or loss is economic or non-economic, quantifiable or non-quantifiable.

Upon such a breach occurring, it should be the duty of the data controller or, on its behalf, the data processor or third party, to provide a breach notification to the individual as soon as possible from the occurrence of the breach as well as take adequate measures to mitigate any harm or damage. The burden of proof to substantiate that adequate measures have been taken should lie with the relevant data controller or data processor or third party. However, if such breach notification is impractical, due to an inability to contact individuals or the substantial number of persons involved, a breach notification may be made by publication in a manner reasonably likely to clearly and unambiguously put such persons on notice of the breach.

For this universe of breaches, notification must be made mandatory as soon as possible after the breach. The future data protection law should clearly stipulate the minimum information that must be included in any breach notifications. We propose that breach notification must at the very least contain the following information:

i. the identity of the data controller, even in cases where the notice is provided by the data processor or a third party;
ii. a general description of the breach
iii. the types of information compromised and the likely consequences of the breach;
iv. the estimated date or range of dates of the breach;
v. the number of individuals involved;
vi. the steps taken to mitigate and remediate the breach;
vii. the individual's rights and the contact information of the entity providing the notice if the persons receiving the notice have any questions;
viii. Steps that individuals can take to respond to the breach

We further note that where a public body responsible for the prevention, detection, or investigation of offences or the future data protection authority determines in writing that such notification of breach will impede a law enforcement investigation, the breach notification may be delayed for the period specified in such written determination.

2. How should a personal data breach be defined?

A breach should be defined to mean *"any unauthorised access, destruction, use, processing, storage, modifications, de-anonymisation, unauthorised disclosure (either accidental, incidental or unlawful) or other reasonably foreseeable risks or data security breaches to personal data transmitted, stored or otherwise processed"*

3. When should personal data breach be notified to the authority and to the affected individuals?

We believe that only those breaches that result in the revealing of categories of sensitive data (as set out in our response to question 1 of this section) and are likely to cause harm to individuals should trigger a breach notification.

Given the sensitive nature of the universe of breaches which would trigger a notification, the data protection authority and every affected individual should be informed of such breaches. Additionally, the steps taken to contain the breach, the steps taken to mitigate the impact of the breach and steps taken to minimise the likelihood of a repeat event should also be communicated to the data protection authority. Breaches that

have high risk of severe adverse impact or harm should be communicated to individuals. Regulators in other jurisdictions have been working on devising classifications for risk and severity for harm.

One such conceptualisation is proposed in the Special Publication 800-30 of the National Institute of Standards and Technology (NIST), USA27. Under this framework adverse impacts include (i) harms to the on-going operations of entity, (ii) the spill-over effects of the breach on operations of other entities, (iii) as well as national security. In this regard, the NIST framework also emphasises that while determining the adverse impact of a data breach, the consequences of the breach on individuals whose data has been compromised must also be considered. These adverse impacts range from financial loss due to compromising of financial data to identity theft, anxiety and reputational damage.

If breach notification to every affected individual is impractical, due to an inability to contact the individuals or the substantial number of individuals involved, a breach notification may be made by publication in a manner reasonably likely to clearly and unambiguously put such persons on notice of the breach.

4. What are the circumstances in which data breaches must be informed to individuals?

We believe that only those breaches that result in the revealing of sensitive data (of the categories set out in our response to question 1 of this section) and are likely to cause harm to individuals should trigger a breach notification. The categories of sensitive data and the definition of harm to be taken into account by entities determining when notifications should be made are set out in our response to question 1 of this section.

5. What details should a breach notification addressed to an individual contain?

A breach notification must at the very least contain the following information:

i. the identity of the data controller, even in cases where the notice is provided by the data processor or a third party;
ii. a general description of the breach
iii. the types of information compromised and the likely consequences of the breach;
iv. the estimated date or range of dates of the breach;
v. the number of individuals involved;
vi. the steps taken to mitigate and remediate the breach;

[27] National Institute of Standards and Technology. (2012, September). Guide for Conducting Risk Assessments. Retrieved January 24, 2018, from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

vii. the individual's rights and the contact information of the entity providing the notice if the persons receiving the notice have any questions;

viii. Steps that individuals can take to respond to the breach

6. Are there any alternative views in relation to the above, others than the ones discussed above?

Chapter 2C: Enforcement Tools and Mechanisms: Categorisation of Data Controllers

1. What are your views on the manner in which data controllers may be categorised?

Different entities that are involved in processing of personal data pose different levels of risk of harm to individuals whose data is being processed. We think there should be some categorisation of data controllers so as to enable differentiated levels of supervision and regulation, for the reasons set out below. Broadly, we believe that data controllers could potentially be categorised into (1) systemically important data entities, (2) normal risk entities, and (3) low risk entities by a future regulator. To do so, a methodology and framework can be developed for the assessment of the level of risk posed by an entity, using quantitative as well as qualitative indicators taking into various factors relevant to the data economy.

Such a categorisation shall enable the future data protection authority to undertake certain enhanced supervisory activities for systemically important data entities so as to mitigate the risk of harm associated with these entities. The enhanced supervisory activities could include a higher frequency and depth of supervision, higher reporting obligations to the future authority, review of data security practices or mandating and reviewing disaster recovery and resolution plans etc. In our view, the law could give an indicating list of such enhanced supervisory activities but should not endeavour to limit such activities.

In the context of data processing, particular entities who aggregate very large volume of personal data related to a very large number of individuals. The size of their databases results in a much larger risk of harm that is associated with such entities. Due to the nature of data itself, very often data systems are heavily interconnected to each other. Thus, a breach in one system could possibly lead to a breach in personal data held by other data controllers. The risk of harm is also dependent on the type of data being processed as well. For example, the harm that can be caused in case an individual's biometric information is leaked can be very high as such information is often used for identity authentication purposes. Considering such variation in the risk of harm posed by various entities, we believe the levels of regulation should also accordingly differ. Such differentiated levels of regulation and supervision can allow for the most optimal use of regulatory capacities and also reduce the burden of compliance for entities which pose a lower level of risk.

In recent years, the financial world has begun evolving an approach to identify financial institutions that are 'systemically important' in nature due to the high level of risk they pose to the financial system as a whole. The developments in this sphere hold relevant learnings for data protection regulation. The Basel Committee of Banking Supervision has created an indicator based assessment methodology, with financial institutions being assessed based on their size, interconnectedness, substitutability, complexity and cross-jurisdictional activities. (Basel Committee on Banking Supervision, 2011) A similar framework could be developed for categorisation of entities which are involved in the processing of personal data.

It must be noted, that in our view, such categorisation should not just be limited to data controllers but extend to data processors as well. In a data ecosystem, the source of a potential breach of data protection is equally likely to be data processor and thus data processors should also be considered within the ambit of such categorisation so as to enable a higher level of regulation to be exercised.

2. Should a general classification of data controllers be made for the purposes of certain additional obligations facilitating compliance while mitigating risk?

As outlined in our response to question 1 above, all entities involved in processing of personal data (i.e. both controllers and processors), should be categorised into (1) systemically important data entities, (2) normal risk entities, and (3) low risk entities, in accordance with a methodology and framework that should be developed to assess the level of risk posed by an entity, using quantitative as well as qualitative indicators taking into various factors relevant to the data economy. Entities which are categorised as "systemically important data entities" under such a framework could be the subject of enhanced supervisory requirements aimed at mitigating the risk of harm posed.

3. Should data controllers be classified on the basis of the harm that they are likely to cause individuals through their data processing activities?

As referred to in our response to question 1 above, the likely harm or risk of harm could be one of the factors included in a future methodology and framework that seeks to assess the level of risk posed by an entity and categorise them into a "systemically important" data entity, "normal" risk entity or "low" risk entity.

4. What are the factors on the basis of which such data controllers may be categorised?

The underlying rationale for categorisation of entities handling personal data is the difference in risk of harm that an entity poses both at the level of a single individual but also in terms of protection of personal data across various interconnected entities across the data ecosystem. The Data Protection Authority should develop a methodology, using both quantitative as well as qualitative indicators, which assess this risk of harm to categorise the entities in the data ecosystem.

The Basel Committee on Banking Supervision has used the following criteria to determine the systemic importance of a bank in the context of the global financial system: (i) size of the bank, (ii) interconnectedness, (iii) substitutability, (iv) complexity and (v) cross-jurisdictional activities. (Basel Committee on Banking Supervision, 2011)

In the Indian financial sector, the RBI Framework for Dealing with Systemically Important Banks also uses the first four of the above criteria to determine which bank should be categorised as systemically important. It must be noted, that the individual indicators that are used by the Bank of International Settlements at the global level and the RBI in India for measuring the respective criteria are different. These factors together help determine the impact that the failure of a particular financial institution shall have on the financial system as a whole, and accordingly modify regulatory actions so as to take higher precautions to prevent such a failure.

Taking note of the criteria that has evolved in the financial sector, there is potential for data regulation to also develop similar thinking and identify core criteria and assessment methodologies. It could potentially use factors such as

- Size of the entity: The volume of data held by an entity is directly linked to the risk of harm that could occur in case of a breach.
- Interconnectedness: The level to which a database is connected to other databases increasing the risk that a breach in one could lead to cascading failures/breach in other data systems. This sort of externalities significantly increases the risk of harm to the data subjects.
- Data types: Certain specific types of data carry a higher risk of harm in case such data is breached. For example, breaches of biometric data of individuals, which are often used for authentication purposes, carry a very high risk of possible harm.
- Data security procedures and protocols: The types of data protection systems that a particular entity has undertaken to safeguard the personal data that it processes have a significant impact on the probability of a breach and subsequent harm to the individual.

It must be noted that the points noted above are merely indicative thinking to demonstrate the potential for such a framework to exist for data regulation. As with the international process in the financial sector, a systematic process and significant amount of analysis would be needed for development of a set of criteria and associated indicators in the realm of data protection.

5. What range of additional obligations can be considered for such data controllers?

Entities which are categorised as systemically important data entities should have certain additional obligations or a higher level of supervision imposed on them. This could include (a) higher frequency and depth of supervision by the Data Protection Authority, (b) higher reporting obligations to the Data Protection Authority, (c) mandating and reviewing data recovery and resolution plans and (d) review of their data security practices, by way of regular audits.

In our view, the data protection law should not limit the range of additional obligations or supervisory actions available to the Data Protection Authority. This must be done so that the authority has the discretion to use the most appropriate tool available and swiftly adapt to changing technologies that are prevalent in the data processing industry. The authority, while exercising the use of various supervisory tools, should take into account various factors like the assessment of the entity carried out during categorisation, nature and seriousness of past violations under the data protection law and response to past supervisory or enforcement directions.

6. Are there any alternative views other than the ones mentioned above?

Registration

1. Should there be a registration requirement for certain types of data controllers categorised on the basis of specified criteria as identified above? If yes, what should such criteria be; what should the registration process entail?

2. Are there any alternative views in relation to registration?

Data Protection Impact Assessment

1. What are your views on data controllers requiring DPIAs or Data Protection Impact Assessments?

Data protection impact assessments can be a useful tool to mitigate the risk of harm in certain scenarios as outlined in the White Paper. DPIAs should be one of tools which the regulatory authority may use in certain scenarios where it is deemed to be an appropriate tool.

2. What are the circumstances when DPIAs should be made mandatory?

3. Who should conduct the DPIA? In which circumstances should a DPIA be done (i) internally by the data controller; (ii) by an external professional qualified to do so; and (iii) by a data protection authority?

4. What are the circumstances in which a DPIA report should be made public?

5. Are there any alternative views on this?

Data Protection Audit

1. What are your views on incorporating a requirement to conduct data protection audits, within a data protection law?

An audit of the data protection practices should be one of the supervisory actions which a future data protection authority may undertake, especially with regard to systemically important data entities. We understand that a data protection audit is typically used to assess an entity's data protection procedures, processes etc. to ensure that such procedures or policies are in place, ensure such processes are adequate and verify that the procedures are being followed. Audits may also be used to highlight potential for failure of compliance and make recommendations to change the procedures in place. (UK Information Commissioner's Office, 2015)

However, before these audits can be conducted clear standards need to be articulated across the market. A future law could include a provision to enable regulators to undertake such audits. In addition, in our view, such data protection audits should be undertaken either directly by the regulatory authority or an independent auditor which is recognised by the authority to carry out such an audit. As mentioned in the response to previous question, the purpose of the audit is to assess the data protection practices of the entity in question. For such an audit to remain credible the auditor in question should be independent in nature from the threats of self-interest, self-review, being in a advocacy position, over-familiarity with elements to be audited and intimidation. (Technical Committe of IOSCO, 2002) These threats to the independence of the auditor must be seriously considered before considering such mechanisms further.

2. Is there a need to make data protection audits mandatory for certain types of data controllers?

3. What aspects may be evaluated in case of such data audits?

4. Should data audits be undertaken internally by the data controller, a third party (external person/agency), or by a data protection authority?

In our view, such data protection audits should be undertaken either directly by the regulatory authority or an independent auditor which is recognised by the authority to carry out such an audit. As mentioned in the response to previous question, the purpose of the audit is to assess the data protection practices of the entity in question. For such an audit to remain credible the auditor in question should be independent in nature from the threats of self-interest, self-review, being in a advocacy position, over-familiarity with elements to be audited and intimidation. (Technical Committe of IOSCO, 2002) In our view, these threats to the independence of the auditor cannot be effectively overcome in the case of an internal audit by the entity.

5. Should independent external auditors be registered / empanelled with a data protection authority to maintain oversight of their independence?

6. What should be the qualifications of such external persons/agencies carrying out data audits?

7. Are there any alternative views on this?

Data Protection Officer

1. What are your views on a data controller appointing a DPO?

A data protection officer can be useful to facilitate compliance with data protection laws within any organisation, especially in organisations which handle large volumes of personal data. Such an officer would also act as an intermediary among the various stakeholders, i.e. a point of contact between the individuals whose personal data is handled and the entity, or the regulatory authority and the entity. Such a point of contact can help in handling grievances that individuals may have with regard to protection of their personal data. In our view, appointment of a data protection officer for a particular entity would be useful to help ensure that entities comply with the provision of the data protection law. (EU Data Protection Working Party, 2016)

Taking into account the potential costs of compliance however, the future regulation would need to allow for mechanisms whereby smaller entities could potentially share services, or use service providers to fulfil this function. Potentially, a progamme of support could also be put in place by the authority to help build the capacity of such organisations. Keeping in mind the potential for the designation of "systemically important data entities" under a future regime, such entities should be mandated to have data protection officers.

2. Should it be mandatory for certain categories of data controllers to designate particular officers as DPOs for the facilitation of compliance and coordination under a data protection legal framework?

As referred to in the response to the previous question, appointment of data protection officers should be mandatory for systemically important data entities (if contemplated by a future data protection regime).

3. What should be the qualifications and expertise of such a DPO?

A DPO should have adequate technical expertise in the field of data collection or processing and the ability to address any requests, clarifications or complaints made with regard to the provisions of the future data protection law. The primary legislation should however not prescribe a set of qualifications for the appointment of data protection officers, as these will need to be set out through more granular regulation, rules or codes taking into consideration the kind of personal data being handled, the volume and complexity of data processing. For example, the qualifications

of the data protection officer suitable for a large social media organisation may not necessarily be suitable for a payments systems company. (EU Data Protection Working Party, 2016)

4. What should be the functions and duties of a DPO?

The functions of the DPO should include at least the following matters:

i. informing and advising the entity for whom they are engaged about the obligations under the data protection regime;
ii. monitoring compliance with the act and the policies of the entity itself in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and related audits;
iii. cooperation and communication with the data protection authority;
iv. responding to complaints and requests from individuals who may contact the DPO on issues related to the processing of their personal data by the relevant entity and to the exercise of their rights under the law.

5. Are there any alternative views?

Chapter 2D: Enforcement Tools and Mechanisms: Data Protection Authority

1. What are your views on the above?

The data protection regime has the two important tasks. First, it must protect and empower individuals' with respect to their personal data. Second, it must provide a secure and stable regulatory framework within which the flow of information can be enhanced. The first aspect is crucial for protecting the fundamental rights and dignity of individuals while the second is a pre-requisite for the growth of the digital economy and continue trading with the rest of the world. Given the sheer volume of personal data that is already being generated, the grave consequence for individuals and huge economic losses for businesses that the misuse of personal information can inflict, it is imperative to create extensive state machinery for continuous and effective data protection.

An independent data protection authority is a crucial element of this machinery.

The independence of the data authority can be insisted for three fundamental reasons:

- *To preserve the principle of 'rule of law'*: The principle of rule of law is the mainspring of administrative law. Rule of law has at least two integral components. On the one hand the rule of law requires that power is not used arbitrarily and the second is a positive requirement that

quasi-judicial and administrative bodies abide by the principles of natural justice (Baxi)[28]. For any regulator to fulfill these requirements, it has to be independent from the government. It is particularly important in the context of data protection, given that the state is also one of the most important users of personal data.

- *To preserve institutional neutrality*: Independence even more valued in the context of data because of the diverse users of data, including the government itself. The independence of the data authority is essential for institutional neutrality. For this reason, the independence of data authority has become a critical indicator of the effectiveness of the data protection regime, worldwide. (Greenleaf, Asian Data Privacy Laws: Trade and Human Rights Perspective, 2014), (Greenleaf, 2018).

- *To meet the global standards necessary for continuing international trade:* Independence of data authority is a critical criteria for meeting the adequacy requirements laid out in the European GDPR (ibid). As of 2017, the EU's share of revenue in the Indian IT sector, was rising and accounted for about $ 50 billion[29]. As is clear from Article 52 of the GDPR, the EU increased emphasis on the independence of the data protection authority of other nations, significantly and this makes the business case for independence of data authority even stronger.

  We reiterate that for the data protection authority to be effective, it will need to be grounded in the theory of responsive regulation and have a range of regulatory sanctions that it can use. The functions of the data protection authority as proposed by the White Paper do not cover all functions that are expected of the authority for effective protection. In addition to the three sets of functions mentioned in the White Paper i.e.– (i) Monitoring, enforcement and investigation, (ii) Awareness generation and (iii) Standard setting, the data protection authority should also be expected to perform the following functions:

- *Coordinate with other regulators, sectoral regulators and public agencies while discharging its functions:* More specifically the data *protection authority can seek information from other regulators, make* references to them for taking corrective action with respect to entities regulated by them and equally, receive recommendations from other regulators regarding corrective actions with respect to data processing practices of entities that may be regulated by them. This can be achieved through signing Memorandums of Understanding (MoU) among regulators[30].

[28] Baxi, U. Developments in Indian Law. In *Public Law in India.*

[29] Economic Times, (November ,2017), How Europe trumped USA for Indian IT companies <https://economictimes.indiatimes.com/tech/ites/how-europe-trumped-us-for-indian-it-companies/articleshow/61633992.cms>

[30] Increasingly it is becoming a practice to sign MoU with each other in order to improve coordination and cooperation. This is seen in Australia's Council of Financial regulator and has been proposed in the draft Indian Financial Code.

- *Reporting of complaints received and enforcement actions undertaken:* The data protection authority is also expected to report its activities with respect to complaints received and enforcement actions taken. The reporting of complaints specifying their nature, scope, geography etc. should happen on a monthly basis, and the reporting of enforcement actions could happen annually.

The functions of the data protection authority are discussed in detail in our response to question 10 of section 2.21, Part IV of the White Paper.

2. Is a separate, independent data protection authority required to ensure compliance with data protection laws in India?

Yes, a separate, independent data protection authority is required to ensure compliance with data protection laws given its vast jurisdiction over the processing of personal data of every resident in India, across sectors and across entities- public bodies and domestic and foreign private entities. The independence of data authorities is increasingly becoming a precondition for cross border data transfers.

3. Is there a possibility of conferring the function and power of enforcement of a data protection law on an existing body such as the Central Information Commission set up under the RTI Act?

No. The Central Information Commission (CIC) has jurisdiction over public authorities excluding intelligence agencies and such public bodies as mentioned in the Second Schedule of the Right to Information Act, 2005. By its design, the CIC cannot monitor, investigate and hold private entities accountable. The future data protection law should extend both to public and private entities, and need a full service regulator to oversee and supervise data practices. For a data protection regime to be effective in prevention of harm to individuals and minimize incidents of data breach, the regulators should also be attentive to ex-ante regulation. Some tools for ex-ante regulations include issuing private warnings, analyzing the complaints database in order to understand emerging pain-points as well as designing methodology for categorization of entities into systemically important entities, medium risk entities and low risk entities and subjecting them to proportionate scrutiny. An effective regulation therefore calls for an extensive regulatory machinery and for these reasons, it is desirable to create a data protection authority and not use an existing institutional set-up for it.

4. What should be the composition of a data protection authority, especially given the fact that a data protection law may also extend to public authorities/government? What should be the qualifications of such members?

5. What is the estimated capacity of members and officials of a data protection authority in order to fulfil its functions? What is the methodology of such estimation?

6. How should the members of the authority be appointed? If a selection committee is constituted, who should its members be?

7. Considering that a single, centralised data protection authority may soon be overburdened by the sheer quantum of requests/ complaints it may receive, should additional state level data protection authorities be set up? What would their jurisdiction be? What should be the constitution of such state level authorities?

8. How can the independence of the members of a data protection authority be ensured?

9. Can the data protection authority retain a proportion of the income from penalties/fines?

10. What should be the functions, duties and powers of a data protection authority?

The data protection authority should be expected to perform nine broad sets of functions. These are outlined below:

(1) **Directions**: The data protection authority may make such directions as required to fulfil its functions under the data protection law, from time to time.

(2) **Advice**: The data protection authority may provide advice to other government agencies, entities including data controllers and processors, or individuals regarding any matters within its jurisdiction.

(3) **Monitoring and research**: The data protection authority shall monitor cross-border transfer of data, security breaches and engage in research regarding the collection, use, disclosure and retention of personal data. Additionally, the authority should update, report and analyse its complaints database. This will help in early detection of data protection issues and allow for ex-ante measures against adverse incidents.

(4) **Supervision and enforcement**:
   (a) Based on the nature and scope of their activities, the data protection authority should design a methodology to classify data controllers and data processors into (i) systemically important entities, (ii) normal entities and (iii) low risk entities.
   (b) The data protection authority is expected to enhance its supervision with respect to systemically important entities. Some tools for higher supervision include reviewing their disaster recovery plans, increasing their reporting obligations and conducting periodic audits.
   (c) With regards to the processing practices of the non-systemically important entities, the data protection authority should encourage inter-sectoral coordination with relevant public authorities and sectoral regulators to operationalise supervisory arrangements.

(d) The data protection authority should maintain complete database of the complaints that it receives and the enforcement actions that it undertakes. Apart from the complaints that it receives directly from consumers, the data protection authority could also issue enforcement actions based on referrals from other public authorities or government agencies; and

(e) The data protection authority should deploy a range of enforcement tools while correcting the behaviour of the regulated entities. These tools include: (1) issuance of a *private warning*; (2) issuance of *informal guidance* in response to a clarification sought by any individual or entity; (3) issuance of a *public statement* (4) issuance of a *show cause notice*; (5) launching of an *investigation* in accordance with the provisions of the data protection law, (6) issuance of a *direction* requiring any individual or entity to remedy any contravention of the provisions of this Act including, but not limited to, compensation, (7) *monitoring compliance* with the orders of the Cyber Appellate Tribunal, where such orders relate to appeals from the orders of the judicial authority; (8) imposition of a *monetary penalty*; (9*) recommendation to relevant public authorities and sectoral regulators* to take such steps as they may be empowered to with respect to any particular individual or entity;

(5) **Investigative functions:** Where the data protection authority has information or reasonable grounds to suspect that any entity is violating or has violated any provision of the future data protection Act, it may investigate such violation by appointing one or more investigators.

(6) **Inter-sectoral coordination**: The data protection authority should take steps to ensure coordination between relevant public authorities and sectoral regulators, in accordance with the provisions of the data protection law. Mechanisms for inter-sectoral coordination include: (1)*requesting for information* from the other authorities in respect of investigations in progress or in connection with enforcement actions; (2) *receiving references or notifications* from other authorities of the contravention of the provisions of the data protection law; (3) *issuing and enforcing enforcement* actions; (4) *recommending enforcement actions* to be undertaken by the other sectoral authorities; (5) *making rules for the coordination* between sectoral authorities including the entry into Memorandums of Understanding between sectoral authorities.

(7) **Adjudication**: The data protection authority shall constitute a judicial authority to adjudicate all disputes and contraventions of the provisions of the data protection law.

(8) **Redressal**: The data protection authority should entertain complaints of individuals with respect to contravention of the data protection law and should l take appropriate steps such as:

(a) promptly sending a notice to the relevant entity seeking reasons for the delay in the resolution of the complaint; and

(b) upon failure to receive an adequate response from the relevant entity within 15 days, taking such enforcement actions against the relevant entity and

(c) provide prompt notification to individuals of the steps taken in order to redress their complaint.

(9) **Reporting**: The data protection authority shall release a report providing aggregate details:

(a) every month, on the complaints received including the number, nature, category, geography, sector and such other factors relating to the complaint as appropriate; and

(b) annually, on the enforcement actions undertaken and complaints it has acted upon.

11. With respect to standard-setting, who will set such standards? Will it be the data protection authority, in consultation with other entities, or should different sets of standards be set by different entities? Specifically, in this regard, what will be the interrelationship between the data protection authority and the government, if any?

Standard setting bodies (SSBs), may be entirely government owned and operated, or can be industry bodies representing industry interests (such as the Payment Card Industry Security Standards Council) or be independent bodies (like the ISO). Since the authority affords protections of not just a right against harm, but also the right to informational privacy, it would be prudent for the Authority to issue standards on its own as well as explicitly approve existing standards of any relevant SSBs as a prerequisite for entities (instead of relying entirely on SSBs or other regulators).

12. Are there any alternative views other than the ones mentioned above?

Chapter 3: Adjudication Process

1. What are your views in relation to an adjudication process envisaged under a data protection law in India?

Yes, the data protection authority should have the power to hear and adjudicate complaints from individuals whose rights have been violated. However, the first point for remedy should be the relevant data controller or data processor. If the data controller or data processor does not act on the individual's complaint or does not act in a manner to the satisfaction of the individual, the individual can approach the data protection authority.

2. Should the data protection authority have the power to hear and adjudicate complaints from individuals whose data protection rights have been violated?

Yes, a quasi-judicial body should be set up to adjudicate on complaints from individuals whose rights under the data protection law have been contravened.

3. Where the data protection authority is given the power to adjudicate complaints from individuals, what should be the qualifications and expertise of the adjudicating officer appointed by the data protection authority to hear such matters?

We propose that the judicial authority should consist of a Chairperson and two members. The selection of Chairperson should be made by the Central Government in consultation with the Chief Justice of India. The members of the judicial authority should be appointed by the Central Government in consultation with the Chairperson.

Further, the judicial authority should consist of at least one judicial and one technical Member. The judicial member should be qualified to be a High Court Judge or have been a member of the Indian Legal Services and held a post in Grade I of that Service for at least three years. A technical Member shall have expertise, special knowledge of and adequate professional experience in technology and processing/collection of data.

4. Should appeals from a decision of the adjudicating officer lie with an existing appellate forum, such as, the Appellate Tribunal (TDSAT)?

No. A separate data protection regulator requires a separate Appellate Tribunal.

Following the Finance Act of 2017, the Cyber Appellate Tribunal envisioned under the Information Technology Act was collapsed and the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) took over its mandate. However, a telecom appellate authority would not be an appropriate forum to consider the wide ranging appeals that will arise in the broad field of data protection. Rather than using the TDSAT, a potential solution could be to refurbish the Cyber Appellate Tribunal structure and have its capacity strengthened, so that it can be a relevant appellate body for issues of data protection.

5. If not the Appellate Tribunal, then what should be the constitution of the appellate authority?

Please refer our response above to question 4 of this chapter.

6. What are the instances where the appellate authority should be conferred with original jurisdiction? For instance, adjudication of disputes arising between two or more data controllers, or between a data controller and a group of individuals, or between two or more individuals.

Yes. The data protection authority should have the powers to adjudicate and offer redress to aggrieved individuals. The determination of monetary compensation must be made after considering the taking the amount of unfair advantage (yielded to the data controller or data processor) as a result of a violation, the amount of harm to the aggrieved person, and the repetitive nature of the violation.

7. How can digital mechanisms of adjudication and redressal (e.g. e-filing, video conferencing etc.) be incorporated in the proposed framework?

Yes. Class action suits in India have been notified under Section 245 of the Companies Act 2013[31] and appear to be particularly relevant in the context of data protection since data breaches affect entire databases which could hold the personal information of scores of individuals. Class action suits can be a useful mechanism to get justice for all individuals whose rights are violated by misuse or unauthorised use of their data.

8. Should the data protection authority be given the power to grant compensation to an individual?

Yes, the authority should be given the power to grant compensation to an individual.

9. Should there be a cap (e.g. up to Rs. 5 crores) on the amount of compensation which may be granted by the data protection authority? What should be this cap?

10. Can an appeal from an order of the data protection authority granting compensation lie with the National Consumer Disputes Redressal Commission?

11. Should any claim for compensation lie with the district commissions and/or the state commissions set under the COPRA at any stage?

12. In cases where compensation claimed by an individual exceeds the prescribed cap, should compensation claim lie directly with the National Consumer Disputes Redressal Commission?

13. Should class action suits be permitted?

Yes. Class action suits in India have been notified under Section 245 of the Companies Act 2013[32] and appear to be particularly relevant in the context of data protection since data breaches affect entire databases which could hold the persona information of scores of individuals. Class action suits can be a useful mechanism to get justice for all individuals whose rights are violated by misuse or unauthorised use of their data.

14. How can judicial capacity be assessed? Would conducting judicial impact assessments be useful in this regard?

[31] Section 245, Companies Act, 2013. Accessible at http://www.mca.gov.in/Ministry/pdf/CompaniesAct2013.pdf, last accessed on 22 January 2018.
[32] Section 245, Companies Act, 2013. Accessible at http://www.mca.gov.in/Ministry/pdf/CompaniesAct2013.pdf, last accessed on 22 January 2018.

15. Are there any alternative views other than the ones mentioned above?

Chapter 4A: Remedies: Penalties

1. What are your views on the above?

The power to impose monetary penalty is a critical enforcement tool available to the prospective data protection authority. Monetary penalties are particularly powerful to incentivise compliance and ensure that the regulated entities continue to remain compliant. An optimum monetary penalty will make compliance to obligations of the law lucrative by adequately penalising the violations of the law. Given that the data protection regime seeks to achieve both, providers' compliance to obligations that will be laid out in the data protection law as well as respect for informational privacy of individuals without causing them harm, monetary penalties are extremely important for ensuring effectiveness of the data protection regime. Penalties are therefore essential to returning the specific violator to compliance and deterring regulated entities from violating.

Proportionality is commonly identified as having three constituent ingredients or stages: rationality (suitability), necessity, and proportionality (Chandrachud, 2013). This will call for means-end analysis as well as balancing of contravention of rights and the amount of penalty, if penalty is found to be suitable. Taking guidance from this approach will allow the prospective data protection authority to account for following factors: (i) the degree of culpability, (ii) any history of prior such conduct, (iii) ability to pay and (iv) effect on ability to continue to do business, when determining the quantum of penalty.

The exact model for penalties i.e. penalising on 'per day basis', 'penalty subject to a fixed upper limit' or 'penalty subject to an upper limit linked to a variable parameter' should be left to the discretion of the adjudicating body and such decisions should be made proportionately.

2. What are the different types of data protection violations for which a civil penalty may be prescribed?

The objective of imposing civil penalties is to disincentivise the regulated entities from acting in a manner that circumvents their obligations under the prospective law. It should also deter them from violating individuals' right to informational privacy as well as not the processing of personal data by regulated entities should not cause harm to individuals.

Keeping the above objectives in mind, determining which specific omissions and violations that attract civil penalties should be left to the discretion of the adjudicating bench. The bench should make such decisions looking at the suitability of penalties as a regulatory action and the quantum of such penalties should be proportionate to the consequences of the contravention. The regulator should consider the entire regulatory spectrum as emphasised in the responsive regulation framework we have laid out in responses to Chapter 1 of Part IV.

3. Should the standard adopted by an adjudicating authority while determining liability of a data controller for a data protection breach be strict liability? Should strict liability of a data controller instead be stipulated only where data protection breach occurs while processing sensitive personal data?

4. In view of the above models, how should civil penalties be determined or calculated for a data protection framework?

5. Should civil penalties be linked to a certain percentage of the total worldwide turnover of the defaulting data controller (for the preceding financial year) or should it be a fixed upper limit prescribed under law?

6. Should the turnover (referred to in the above question) be the worldwide turnover (of preceding financial year) or the turnover linked to the processing activity pursuant to a data protection breach?

7. Where civil penalties are proposed to be linked to a percentage of the worldwide turnover (of the preceding financial year) of the defaulting data controller, what should be the value of such percentage? Should it be prescribed under the law or should it be determined by the adjudicating authority?

8. Should limit of civil penalty imposed vary for different categories of data controllers (where such data controllers are categorised based on the volume of personal data processed, high turnover due to data processing operations, or use of new technology for processing)?

No, limits on civil penalties should not be conditional to categorisation of data controllers, per se. However, the ability to pay of the faulting entity may be factored in while determining the quantum of penalties. There is some precedence of using ability to pay principle in other jurisdictions while determining the quantum of penalty. The American Department of Environmental Protection, for instance factors in this dimension while determining civil penalties. As per guidance to the states, the Department is advised to factor in the financial health of the violator- usually by the presentation of accurate financial records of the last three to six years. The Department is also advised on calculating if the future cash flows of the violator will be adequate for continuing business if the penalty has been paid off. (United States Environmental Protection Agency, 1986).[33]

[33] United States Environmental Protection Agency. (1986). *Memorandum: Guidance on Determining a Violator's Ability to Pay a Civil Penalty, December 16, 1986.* Washington D.C.: Environmental Protection Agency.
https://www.epa.gov/sites/production/files/documents/civilpenalty-violators.pdf

Therefore, the civil penalties should take into account the unique circumstances of the violator like if the penalty will interfere with their financial ability to come into compliance or reasonably be expected to force the violator out of business. However, no pre-defined categorical limits may be established.

Other factors that should be considered include the: (i) the degree of culpability, (ii) any history of prior such conduct.

9. Depending on the civil penalty model proposed to be adopted, what type of factors should be considered by an adjudicating body while determining the quantum of civil penalty to be imposed?

The determination of civil penalties should be proportionate to the consequences of the contravention guided. Guidance can be taken from the legal conception of proportionality that has three components- (i) rationality (or suitability), (ii) necessity and (iii) proportionality. (Chandrachud, 2013) The rationality strand guides in assessing the appropriateness of the penalty in achieving the desired regulatory outcome, the necessity test tests the need for the penalty and proportionality is the test of balancing.

More specifically factors that can be considered while determining the quantum of penalty are (i) account the degree of culpability, (ii) any history of prior such conduct, (iii) ability to pay, (iv) effect on ability to continue to do business.

The proposed data protection authority should explore the suitability of a broader menu of enforcement actions, grounded in the theory of responsive regulation, while determining an enforcement action.

10. Should there be a provision for blocking market access of a defaulting data controller in case of non-payment of penalty? What would be the implications of such a measure?

11. Are there any alternative views on penalties other than the ones mentioned above?

Chapter 4B: Remedies: Compensation

1. What is the nature, type and extent of loss or damage suffered by an individual in relation to which she may seek compensation under a data protection legal regime?

2. What are the factors and guidelines that may be considered while calculating compensation for breach of data protection obligations?

The compensation rewarded to the injured parties should be proportionate to:

(1) The unfair advantage afforded to the service provider, because of contravention on part of the provider,

(2) the amount of harm to any individual, and

(3) the repetitive nature of the default;

While assessing the harms suffered, the adjudicating authority may take into account not only the direct losses that have been sustained by the injured party but also the profits that have been foregone. Given that the remedy of compensatory damages is grounded in the equalisation theory and is seen as a measure to restore the injured party to their former position, compensation for foregone profits as well as direct losses is an acceptable position of the law. (Demogue, 1918)[34] The Indian Financial Code also provides for considerations[35] for losses sustained, profits foregone as well as the material distress or material losses sustained on account of the wrongdoing of the financial service provider.

Moreover, in the context of personal, all harms may not manifest at once or they may be of a recurring nature. Such considerations should also be factored in while providing for relief.

As recognised in the White Paper, not all harms are quantifiable or economic in nature. The adjudicating authority should be sensitive to the non-economic harms as in other jurisdictions (like the EU and South Africa), as cited in the White Paper.

Given that the proposed data protection law applies uniformly to both public and private data controllers and processors, the remedy of compensation should be exactable from all data controllers regardless of their ownership.

3. What are the mitigating circumstances (in relation to the defaulting party) that may be considered while calculating compensation for breach of data protection obligations?

The mitigating circumstances are directly related to the liability standard that providers are held up to. Breach of data protection that occurs because of providers not upholding their obligations as laid out under the proposed law will attract strict liability.

The consent of the injured party should not be a mitigating circumstance in the context of privacy and personal data. The limitations of consent have been effectively established in literature[36] and have been widely recognised in Chapter 1 of Part III of the White Paper. Due to information asymmetries, psychological distortions like immediate gratification and inadequate understanding of the risk to privacy due to sharing their personal data, the role of consent has changed significantly. It is no longer an instrument of providing informed and valid permission to a data controller, allowing them collection of personal data. Today, consent is merely a tool of information made available to the individual when their

[34] Similar principle is found in the Italian Civil Code, the Venezuelan Civil Code, the Dutch Civil Code- for a nuanced discussion see: Demogue, R. (1918). Validity of the Theory of Compensatory Damages. *The Yale Law Journal*, 585-598.
[35] Section 132(4) of the Indian Financial Code.
[36] (Acquisti, 2004)

personal data is being processed. Understanding the invalidity of consent as a legal tool, consent should not be used as a mitigating circumstance in the case of data protection.

Mitigating circumstances that may be applicable in the context of breach of data protection could include Act of God i.e. natural calamities or incidents beyond the control of human agency.

4. Should there be an obligation cast upon a data controller to grant compensation on its own to an individual upon detection of significant harm caused to such individual due to data protection breach by such data controller (without the individual taking recourse to the adjudicatory mechanism)? What should constitute significant harm?

5. Are there any alternative views other than the ones mentioned above?

Chapter 4C: Remedies: Offences

1. What are the types of acts relating to the processing of personal data which may be considered as offences for which criminal liability may be triggered?

2. What are the penalties for unauthorised sharing of personal data to be imposed on the data controller as well as on the recipient of the data?

3. What is the quantum of fines and imprisonment that may be imposed in all cases?

4. Should a higher quantum of fine and imprisonment be prescribed where the data involved is sensitive personal data?

5. Who will investigate such offences?

6. Should a data protection law itself set out all relevant offences in relation to which criminal liability may be imposed on a data controller or should the extant IT Act be amended to reflect this?

7. Are there any alternative views other than the ones mentioned above?

BIBLIOGRAPHY

Acquisti, A. (2004). *Privacy in Electronic Commerce and the Economics of Immediate Gratification*. Proceedings of the 5th ACM Conference on Electronic Commerce, 21-29.

Acquisti, Alessandro and Grossklags, Jens. (2007), *What can Behavioural Economics teach us about Privacy?* Digital Privacy: Theory, Technologies and Practices. Taylor and Francis Group.

Acharya, Bhairav. (2015). *The Four Parts of Privacy in India.* Economic and Political Weekly, Vol. L No.22.

Alsenoy, B. V. (2017). *Liability under EU Data Protection Law*. Jipitec 271.

Australian Communications and Media Authority. (2011). *Optimal Conditions for Effective Self- and Co-Regulatory Arrangements*. Melbourne: Australian Communications and Media Authority.

Basel Committee on Banking Supervision. (2011). *Global Systemically Important Banks: Assessment Methodology and additional loss absorbency requirement.* Bank of International Settlements.

Calabresi, G. (1970). *The Cost of Accidents: A Legal and Economic Analysis*. New Haven; London: Yale University Press.

Calo, R. M. (2012). *Against Notice Skepticism in Privacy*. Notre Dame Law Review, 1027.

Chandrachud, A. (2013). *Wednesbury Reformulated: Proportionality and the Supreme Court of India*. Oxford University Commonwealth Law Journal, 13 (1), 191-208.

Chugh, B and Raghavan, M. (2017, October). *Moving towards a user data rights regime*. Mint, Retrieved from http://www.livemint.com/Opinion/6bNi3LnWTH2JWEpZmSuuBI/Moving-towards-a-user-data-rights-regime.html.

Comandé, G. (2017). *Regulating algorithms regulation: First ethico-legal principles, problems and opportunities of algorithms.* In D. Q. Tania Cerquitelli, Transparent Data Mining for Big and Small Data. New York: Springer International.

Consumer Affairs Victoria (2006). *Consumer detriment in Victoria: a survey of its nature, costs and implications.* Research Paper No. 10 October 2006. Retrieved from: https://www.consumer.vic.gov.au/library/publications/resources-and-education/research/consumer-detriment-in-victoria-a-survey-of-its-nature-costs-and-implications-2006.pdf.

CGAP, Dalberg and Dvara Research. (2017). *Privacy on the line.* Retrieved from http://foundation.ifmr.co.in/wp-content/uploads/2017/11/Privacy-On-The-Line.pdf

Demogue, R. (1918). *Validity of the Theory of Compensatory Damages.* The Yale Law Journal, 585-598.

DiGangi, C. (2017). *What is a Schumer Box?* Retrieved from: https://www.credit.com/credit-law/what-is-a-schumer-box/.

Eisenberg, , J. N., & K&L Gates . (2016, January 24). *Calculating SEC Civil Money Penalties.* Retrieved January 17, 2018, from Harvard Law School Forum on Corporate Governance and Financial Regulation: https://corpgov.law.harvard.edu

European Commission (2017). *Study on measuring consumer detriment in the European Union*. Retrieved from: http://ec.europa.eu/consumers/consumer_evidence/market_studies/docs/consumer_detriment_study_final_report_part_1_main_report_en.pdf.

European Union Agency for Network and Information Security. (2014). *Privacy and Data Protection by Design – from policy to engineering, December 2014.* Retrieved from: https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2015/01/Privacy-and-Data-Protection-by-Design.pdf

EU Data Protection Working Party. (2010). *Opinion on concepts of 'controller' and 'processor'*.

EU Data Protection Working Party. (2016). *Guidelines on Data Protection Officers*.

Greenleaf, G. (2014). *Asian Data Privacy Laws: Trade and Human Rights Perspective*. London: Oxford University Press.

Greenleaf, G. (2018). *Data Protection: A Necessary Part of India's Fundamental, Inalienable Right to Privacy: Draft Submissions on the White Paper of the Committee of Experts On a Data Protection Framework in India*. Retrieved from https://ssrn.com/abstract=3102810

Koops, B.-J. (2017). *A Typology of Privacy*. University of Pennsylvania Journal of International Law, 484-575. Retrieved from: https://pdfs.semanticscholar.org/fe72/a06daf70f03ba5713b529f60c900d5f2564c.pdf.

Leonard, P. (2014). *An Overview of Privacy Law in Australia: Part 2*. Communications Law Bulletin, Vol 33.2 (June 2014). Retrieved from: http://www.austlii.edu.au/au/journals/CommsLawB/2014/6.pdf

McGeveran, W. (2016). *Friending the Privacy Regulator*. Faculty Articles, University of Minnesota Law School.

Merz J.F., Fischhoff B. (2009). *Informed consent does not mean rational consent*. Retrieved from https://goo.gl/wJD5k9

Moerel, L., & Prins, C. (2016). *Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things* (May 25, 2016). Retrieved from: https://ssrn.com/abstract=2784123 or http://dx.doi.org/10.2139/ssrn.2784123

Nissenbaum, Helen. (2004). *Privacy as Contextual Integrity.* Washington Law Review.

Office of Australian Information Commissioner. (2013, September). *Guidelines for Developing Codes: Issued Under Part III-B of the Privacy Act of 1988*. Melbourne, Sydney, Australia.

Priest, M. (1997-98). *The Privatisation of Regulation: Five Models of Self Regulation*.

Raghunathan, B. (2013). *The Complete Book of Data Anonymisation: From planning to implementation*. CRC Press.

Rubinstein, I. S. (2010). *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*. Journal of Law and Policy for the Information Society, 355-423.

Sarathi, Vepa P (2005). *Interpretation of Statutes*.

Schaub, F. et. al. (2015), *A Design Space for Effective Privacy Notices.* USENIX Association, 2015 Symposium on Usable Privacy and Security. Retrieved from: https://www.ftc.gov/system/files/documents/public_comments/2015/10/00038-97832.pdf

Shavell, S. (1982). *On Liability and Insurance*. The Bell Journal of Economics, 13(1), 120-132. doi:10.2307/3003434

Sinclair, D. (1997). *Self- regulation versus command and control? Beyond false dichotomies*. Law & Policy, 19(4), 529-559.

Solove, D. J. (2012). *Privacy self-management and the consent dilemma.* Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018

Solove, D. J., & Citron, D. K. (2017). *Risk and Anxiety: A Theory of Data Breach Harms*. GWU Law School Public Law Research Paper No. 2017-2; GWU Legal Studies Research Paper No. 2017-2. Retrieved from: https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2499&context=faculty_publications

South Africa. South African Law Reform Commission. (2005). *Privacy and Data Protection: Discussion Paper 109, Project 124*, October 2005 (ISBN 0-621-36326-X). Pretoria: South African Law Reform Commission. Retrieved from: http://www.justice.gov.za/salrc/dpapers/dp109.pdf.

Technical Committee of IOSCO. (2002). *Principles of Auditor Independence*. International Organisation of Securities Commissions.

UK Information Commissioner's Office. (2014). *Data Controllers and Data Processors*.

UK Information Commissioner's Office. (2015). *Auditing Data Protection: A guide*. UK Information Commissioner's Office.

US Federal Communications Commission (2017). *Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission*, Submitted to the Federal Communications Commission, 27 May 2016. Retrieved from: https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf.

U.S. Federal Deposit Insurance Corporation (2017). *FDIC Compliance Examination Manual – March 2017, II. Compliance Examinations - Evaluating Impact of Consumer Harm*. Retrieved from https://www.fdic.gov/regulations/compliance/manual/2/ii-2.1.pdf.