Response to the White Paper on a Data Protection Framework for India

Vrinda Bhandari Advocate

Amba Kak Mozilla Foundation

Smriti Parsheera **Faiza Rahman** **Renuka Sane** National Institute of Public Finance and Policy

We thank the Committee for the opportunity to provide our inputs on the formulation of a data protection framework in India. We support the idea of a principles-based data protection law with a strong institutional framework for the formulation of regulations to supplement the principles laid down in the the law; enabling effective monitoring and enforcement; and appropriately addressing the complaints raised by individuals in relation to any breach of their data protection rights.

The scope of the data protection law should extend to all sectors and all entities that collect and process user data, whether in the public sector or the private sector. Nevertheless, a one-size-fits-all model seems ill suited given the variations in the nature and uses of different types of data in the hands of different categories of data controllers and the potential harms that could result from it. This makes it essential to ensure that the principles in the law are not drafted in a manner that is designed to address the needs or potential concerns emanating from particular categories of stakeholders or specific uses of data. We recommend that the nuances of different situations be built into context-specific and sector-specific subordinate legislation.

The data protection law must therefore focus on the identification of the key areas where more specific regulations need to be framed and the legal process to be followed by the agencies implementing the law. This will include the requirement to follow a consultative and transparent process while drafting regulations and adherence to the rule of law while investigating and implementing the provisions contained in the law and regulations.

Taking into account these objectives, we propose the establishment of two new agencies under the data protection law:

1. A Data Protection Authority (DPA) that will function as a cross-sectoral privacy regulator, with legislative powers (drafting regulations that are binding on regulated entities), executive powers (in its supervision and monitoring activities) and quasi-judicial functions (assessing compliance with the law by regulated entities and initiating enforcement actions); and

2. A Data Protection Redress Authority (DPRA) that will be responsible for adjudicating individual complaints and affording appropriate remedies for any breach of the data protection rights of individuals.

The rationale for setting up two separate agencies, and their specific roles and functions are explained in further detail in our responses below. Many of the suggestions made by us draw from the recommendations of the Financial Sector Legislative Reforms Commission (FSLRC), an expert body headed by Justice B.N. Srikrishna that was tasked with the comprehensive review of all financial sector laws in India.[1] The committee on data protection could benefit greatly from the recommendations of the FSLRC and the draft Indian Financial Code drafted by them, particularly on the issues relating to the design and functioning of the DPA and DPRA and allocation of responsibilities between them.

While the focus of our submissions remains on issues of regulatory structure and agency design (**page 22 onwards of this submission**), we are also providing our selective inputs on some of the other questions posed by the Committee in its White Paper.

PART I - SCOPE AND EXEMPTIONS

DEFINITION OF PERSONAL DATA

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

The definition of personal data should include both identified or reasonably identifiable information relating to an individual. The contours of what qualifies as "reasonably identifiable" personal data will evolve rapidly with the evolution of technologies. For instance, a study in United States found that 87.1 percent of the people were uniquely identified by their combined five-digit ZIP code, birthdate and sex (Sweeney, 2010). Another study re-identified data subjects based purely on their movie preferences on Netflix (Arvind Narayanan et al, 2008). Thus, the science of what data fields might lead to re-identification when combined with other fields (and even other available databases) is an evolving one, necessitating a broad view of the definition of personal data or information.

We recommend a concerted effort to publish guidelines and consultations on what fields of data, in what contexts, are *likely* to combine to reveal personal data. The emphasis should be on recognising combinations of fields of data that are likely to disclose personal data.

[1] The FSLRC report and the draft Indian Financial Code are available at report http://dea.gov.in/fslrc.

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

We believe that the use of either term - "personal data", or "personal information", in the data protection law works, as long as the term can be defined to mean identified or reasonably identifiable information relating to an individual.

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?

Defining the term personal data is integral to providing certainty to regulated entities on the scope of their obligations. It is the ability of personal data to be traced back to a particular individual, and consequently, potentially impact their autonomy and dignity that makes it the bedrock of data protection regimes globally.

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?

The definition of personal data should include identified, identifiable and 'reasonably identifiable' data, for the reasons outlined above.

Should anonymised or pseudonymised data be outside the purview of personal data? Should the law recommend either anonymization or pseudonymisation, for instance as the EU GDPR does?

It is reasonable to exclude anonymised and pseudonymised data that meets an acceptable standard of de-identification. However, such exclusion would only apply to the extent that such information is not captured by the "reasonably identifiable" clause in the definition of personal data. As explained above, the understanding of what counts as reasonably identifiable will evolve to keep pace with state of the art research. As such, certain anonymised data (in combination with other data or otherwise) and even pseudonymised data may be included under the definition of personal data if techniques of pseudonymisation or anonymisation are not robust enough to prevent re-identification of individuals.

Should there be a different level of protection for data where an individual is identified when compared to data where the 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?

The standard should be the same. The basis for protecting personal data is the *ability* of such data to be traced back to the individual, and technologies make this ability indistinguishable for practical purposes.

SENSITIVE PERSONAL DATA

What are your views on sensitive personal data?
Should the law define a set of information as sensitive data? If yes, what category of data should be included in it?

The definition of sensitive data is unarguably complex. As noted privacy scholar Professor Nissenbaum has highlighted, sensitivity depends more on context than on the data type in question (H. Nissenbaum, 2004). Despite the highly subjective nature of what constitutes sensitive data, we think there is value to a regulatory regime that recognises certain data types as especially sensitive with the consequence of stricter requirements that may not be imposed on all data controllers, especially when the baseline protection for all other personal data is high.
The test for classifying certain information as sensitive personal data should be based on a expectation of the likely harm that could be reasonably caused to the individual in case of a breach of the requirement to protect that data.

Apart from the categories mentioned by the Committee, we recommend that biometric data (such as iris scans, DNA, and fingerprints) should also be treated as sensitive personal data. Having such a list of sensitive data will provide legal certainty to data controllers that there are certain types of data that need to be subject to stricter care due to their capacity to harm. While such a list is not an end in itself, it functions as a useful "rule of thumb" that puts the data controller on high alert (Ohm, 2014).

However, we would caution against any approach that might seek to limit the effective scope of the data protection law only to a limited category of sensitive personal data. Instead, it should be used for the purpose of imposing *stricter* requirements in particular circumstances. This may include the need for more stringent data security measures, audit requirements, emphasis on informed consent in the collection and processing of the information, and linking breaches/leaks of such sensitive data to higher penalties (to create effective deterrence, and encourage companies to improve their data security measures). Derogations from consent to "other grounds of processing" should be extremely limited when it come to sensitive personal data.

Finally, this list must be an evolving one, with an obligation on the DPA to review and make additions or adaptations (in specific contexts) to the categories of sensitive personal data, as the outcome of a consultative process.

DEFINITION OF DATA CONTROLLER AND PROCESSOR

What are your views on the obligations to be placed on various entities within the data ecosystem?
Should the law only define data controller or should it additionally define data processor?
How should responsibility among different entities involved in the processing of data be distributed?
Are there any other views on data controllers or processors which have not been considered above?

As noted by the Committee in the White Paper, a number of different entities are involved in the life cycle of collection, use and processing of data. Each of these entities plays a different role in the data cycle and should accordingly be bound by different levels of responsibilities in the data protection framework. It is therefore important to separately define the terms "data controller" and "data processor".

In terms of allocation of responsibilities, we are of the view that the data controller, which is the entity that either collects or determines the purpose for which the data is to be used, should be primarily responsible for adhering with the requirements of the law. In situations where the controller utilises the services of any third party, the controller would be required by the law to ensure that the processor has the capacity and appropriate mechanisms to ensure adequate protection of the data in accordance with the law.

In terms of enforcement actions and attribution of liability, we propose that the following distinction should be made between data collectors and processors:
(i) In case of a complaint raised by an individual before the DPRA, the individual would have recourse against the data controller with whom she shares a relationship, even if the violation takes place due to an act by a data processor. This will ensure that the individual is not put under the burden of determining which specific entity in the data cycle is responsible for a particular breach.

The controller can safeguard itself from liabilities arising from such claims by putting in place appropriate checks while selecting the data processor and through appropriate contractual arrangements, including indemnity provisions.

(ii) Data processors would however be subject to the supervision of the DPA, which may frame appropriate regulations to specify the obligations of data processors and initiate enforcement actions against the data processors for any violation of those requirements.

EXEMPTIONS FOR HOUSEHOLD PURPOSES, JOURNALISTIC AND LITERARY PURPOSES AND RESEARCH

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

The chapter on exemptions in the White Paper focuses on the types of activities that may be exempted from data protection principles, for instance it states that exemptions may be granted for data processed for domestic/household purposes, national security, literary/artistic purposes etc. However, the White Paper does not highlight the manner in which the legitimate applicability of such exemptions shall be established. We propose that the requirements of necessity and proportionality should be embedded within the provision that sets out the various activities exempted from data protection principles.

The Supreme Court in *Puttaswamy v. Union of India* held that the state may have an interest in placing reasonable limits on informational privacy in the interest of legitimate aims such as protecting national security, preventing and investigating crime, encouraging innovation, and preventing the dissipation of social welfare benefits. However, apart from indicating the broad parameters of such exemptions, a majority of the judges (Chandrachud J speaking for 4 and Kaul J) have also held that the European concept of proportionality will be used to balance the right to privacy and competing interests. Chandrachud J., notes that any invasion of life or personal liberty must satisfy the following three requirements of the proportionality test:

- legality, i.e. there must be a law in existence;
- legitimate aim, which he illustrates as including goals like national security, proper deployment of national resources, and protection of revenue; and
- proportionality of the legitimate aims with the object sought to be achieved.

Kaul J.'s adds to this a fourth element of "procedural safeguards against abuse of interference with rights", which echoes Article 21's central requirement of having a "procedure established by law".

Further data protection frameworks across many jurisdictions and international human rights instruments adopt this approach wherein the law uses the proportionality principle coupled with specified activities to set out the exemptions to principles of data protection or privacy. For instance Article 23 of the GDPR states:

"*Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22,* ***when such a restriction respects the***

essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard*:*
(a)national security
(b)defence…."

Similarly, Article 8 of the European Convention of Human Rights marries the proportionality approach with the restrictions on the right to privacy by stating:
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except ***such as is in accordance with the law and is necessary in a democratic society in the interests of*** national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

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

Exemptions, even when reasonable and non-arbitrary, should not be entirely absolve entities from data protection obligations. We agree with the Committee's view to mandate exempted activities to still comply with adequate security and organisational measures for protecting data against unauthorised access. This may include requirements relating to encryption of personal data, mandatory issuance of data breach notifications and other security requirements, as may be detailed under regulations. In addition, the law should also lay down an obligation to devise an effective review mechanism for such security guidelines.

ALLIED LAWS

Comments are invited from stakeholders on how each of these above laws, or any other relevant law not listed above, may need to be reconciled with the obligations for data processing introduced under the new data protection law

We are of the view that a legal analysis of the exact changes that will need to be introduced in all the allied laws mentioned in this chapter can only be done effectively once we have better clarity regarding the expected shape of the final law. However, we believe that the principle commitments of this data protection legislation such as collection limitation, purpose limitation, proportionality must definitely be reflected in all the allied laws.

As an example, we demonstrate below the manner in which the commitment of proportionality needs to be reflected in the Indian Telegraph Act, 1885.

The current framework for lawful interception under the Indian Telegraph Act,1885 (Telegraph Act) was held to be constitutional by a two judge bench of the Supreme Court in **PUCL v. UOI** (1997) subject to the adoption of appropriate procedural safeguards. This led to the subsequent amendment of the Telegraph Rules to incorporate the procedure suggested by the Supreme Court. At present, Section 5(2) of the Telegraph Act, read with Rule 419A of the Telegraph Rules, 1951, empowers the state to conduct lawful interception activities. Section 5(2) states that the Central or State Government, or any officer specially authorised by them may direct the interception of communications under certain specified circumstances. Rule 419A authorizes the Secretary to the Ministry of Home Affairs in the case of Central Government and the Secretary the Home Department in the case of a State Government to issue the orders of interception.

We submit that it has become critical to reexamine the interception provisions of the Telegraph Act in light of the Supreme Court's nine judge bench decision in the Puttaswamy case, primarily for the following reasons:

- Significant time has lapsed since the passage of the PUCL decision. In this time, the capability of surveillance and interception technologies at the disposal of any government and the volume of interception being carried out have increased exponentially meriting a re-look at the existing procedures.
- The Telegraph Act and rules were drafted in a context when bulk surveillance was not as easily possible. Since then the Government has announced the setting up of the Centralised Monitoring System (CMS) and made corresponding changes to telecom licenses to provide real-time access to the traffic flowing through their networks to facilitate lawful interception of communication. However, sufficient details pertaining to the nature of the CMS framework and the procedural safeguards against infringement of privacy that are being built into it, are not available in the public domain.
- A report prepared by SFLC[2] reports that nearly 7500 to 9000 interception requests are approved just by the Central Government on a monthly basis. Applying the "proportionality" and "due process" tests laid down under the Puttaswamy decision to these facts would lead one to question whether the current procedures allow for due application of mind, given the high volume of interception requests being made to the Secretary.
- Lastly, as stated above, the PUCL case that examined these provisions was a two judge bench of the Supreme Court. Now that a higher bench comprising nine judges has held that going forward all restrictions on right to privacy will be tested against the rigorous standard of proportionality, interception provisions in the Telegraph Act will also need to satisfy the new tests laid down by the Supreme Court.

[2] https://www.sflc.in/indias-surveillance-state-our-report-on-communications-surveillance-in-india

Therefore, we recommend that there is a need to revisit the interception architecture set out under the Telegraph Act. Specifically, any attempts to amend the provisions under Telegraph Act should tailor such amendments to meet the legitimate aim and proportionality tests set out in the Puttaswamy judgement.

PART II - GROUNDS OF PROCESSING, OBLIGATION ON ENTITIES AND INDIVIDUAL RIGHTS

CONSENT

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 are of the view that consent should remain a fundamental ground for the collection, use and disclosure of personal data. However, the law will also need to recognise other permitted grounds such as lawful requirements and legitimate business purposes. In the latter case the onus would be on the data controllers to establish the direct nexus between the legitimate purpose and the nature of data processing being undertaken, both to the data subject and the DPA.

Further, instead of using the term “processing” to refer to the different types of data activities, it would be useful to draw a distinction between the different stages of data processing so as to require data controllers and processors to identify the appropriate standards of consent and the permissible alternatives to consent at each stage.

For instance, different types of consent requirements may be applicable at the point of collection of information -- where the user is more likely to be aware of and understand the immediate purpose for which the data will be utilised -- versus subsequent sharing of the information with an affiliate or third party, where a separate consent may need to be taken at the relevant point of time. The requirements at each stage will also vary depending upon the specific context. Therefore we propose that the primary law should lay down the requirement of consent and the principle that consent has to be obtained in an informed and meaningful manner. Further details in this regard should be formulated by the data collectors while complying with the principle and the DPA by framing appropriate regulations.

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?
How can consent fatigue and multiplicity of notices be avoided? Are there any legal or technology-driven solutions to this?
Would having very stringent conditions for obtaining valid consent be detrimental to day-to-day business activities? How can this be avoided?

Yes, the law should lay down the principle that consent needs to be provided in an informed and meaningful manner. Admittedly, there will be several complexities in the effective translation of this principle into practice but these challenges should not be seen as a ground for abandoning or diluting the requirements of consent. Data collectors should rely on simplified notice conditions as one of the tools for facilitating meaningful consent.

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

It is essential to ensure that the principles in the law are not drafted in a manner that is designed to address the needs or potential concerns emanating from particular categories of stakeholders or specific uses of data. For instance, the context-setting chapter of the white paper highlights the rapid advances in technology, creation of new digital markets and the resulting benefits and challenges of big data. While these are all relevant issues, a comprehensive, cross-sectoral data protection law must equally account for the protection of data exchanges in other traditional settings, which may not necessarily be driven by digital or information technology based processes. This would include sharing of data by the data subject with educational institutions, employers, medical care providers, etc. Consent remains an essential requirement in all these contexts.

The principle of consent should therefore be drafted in a manner that allows data collectors to make context-specific determinations. However, this should be done within the bounds of the other requirements set out by the law and the regulations framed by the DPA.

NOTICE

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

Proper notice is an essential requirement for operationalising effective consent and we recommend that this should be mandated in the law. However, the notice and consent regime

must not be treated as the sole, or even primary mechanism, for ensuring privacy protections. This should instead be achieved through a combination of factors, as suggested below.

Firstly, the law should first adopt the principle of "privacy by design", which implies that privacy requirements should be taken into account at every stage of the design of a new system and privacy enhancing techniques should be treated as the default option.

Secondly, the law should contain the principle that privacy notices must be provided in a form and manner that is suitable for the requirements of the data subject and enables them to provide their meaningful and informed consent. In order to be meaningful, the notice should be given in a manner and at a time that would inform a reasonable user in the position of the data subject regarding the data processing permissions being sought and the purpose of the same. The data controller would, however, not be required to ensure that each and every individual does in fact understand all the information being shared in the notice as that would be too onerous a requirement. The DPA may assess the privacy notices issued by data controllers to ensure that this principle is being adequately complied with.

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?

The requirement to share information regarding the data processing practices followed by them should apply equally to private and government data controllers. At present, many stakeholders try to provide adequate notice to individuals through a complex set of terms and conditions. These terms are generally crafted in legal language, which is not comprehensible to the general audience. The objective in such cases is generally to disclaim future legal liability rather than to genuinely inform the data subject. In order to avoid this, we recommend that data collectors and processors should be bound by a robust set of privacy principles and accountability obligations, over and above the notice and consent regime.

In addition, various mechanisms can be considered for making privacy notices more comprehensible to individuals. This may include requirements of *layered notice*, where a set of key terms about the privacy policy are declared upfront in a summarised manner with the option for the individual to read through the more detailed terms. Another option is to require all data collectors to display *standardised icons* that can simplistically convey key information, such as: Does the site share personal information with third parties? Does the site engage in behavioural targeting? How long does the site retain personal information?[3]

[3] Guidelines for Online Consent, Office of the Privacy Commissioner of Canada, see https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_oc_201405/.

The law should empower the DPA to test these and other similar tools for facilitating better notice to individuals and create a framework for their adoption by data collectors. In limited circumstances the DPA could also mandate the adoption of such tools for particular categories of data controllers, subject to the compliance with the regulation making processes suggested later on in our submission.

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

Privacy impact assessments can serve as a valuable tool for assessing the privacy implications of a system, both prior to its launch and on an ongoing basis. However, we would not recommend making a provision in the law to make such an impact assessment exercise mandatory for *all* data controllers. There will however be some situations where such an exercise would be considered to be desirable based on the volume of data being collected by an entity, the nature or sensitivity of the data or the potential harm that could result from it. Therefore, we recommend that the DPA and sectoral regulators, where applicable, should have the legal authority to mandate certain categories of data collectors or even specific collectors to conduct privacy impact assessments.

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 not support the idea of having detailed form based prescriptions of privacy notices in the primary law. The law should identify the broad categories of information that need to be provided to the data subject, such as, details of the data collector, types of data being collected and its uses, the manner and purpose for which data may be shared with affiliates or third parties, etc. Where relevant, more detailed requirements may be prescribed by the DPA and/or sectoral regulators, if applicable.

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?

The purpose of the notice and consent requirement should be to inform users rather than to absolve the data collector from any future liabilities. Therefore, the notice and consent provisions should be drafted as standalone requirements in the law, with clear consequences for any non-compliance. The provision of such notice should not be linked to any dilution of the other protections given to data subjects or to operate as a safe harbor for data collectors. It would however be one of the relevant factors taken into account by the DPA or the DPRA while looking into any allegations of investigations against the data collector.

The provisional views of the committee refer to the adoption of a 'data trust score' which would be similar to credit scores. Pending further information regarding the proposed design of such a mechanism, we would like to highlight a few points that may be taken into account. The exercise of assigning data trust scores to all data collectors would be a mammoth exercise requiring significant time and resources. Therefore, we do not recommend that this task should be carried out by the DPA, which should focus instead on its core functions of regulation and supervision. This function may be performed by other third party entities, in which case it will also be necessary to monitor the trustworthiness and incentive structures of the scoring entities themselves. This may require some form of supervision of such entities by the DPA or some other body.

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?

Individuals would benefit greatly from the availability of a consent dashboard that provides a snapshot of the privacy permissions given by them to various data controllers. Such a service can be provided by multiple third parties based on commercial arrangements entered into with individuals. In such a case the individual would provide the dashboard operator with information about each product or service availed by her and the dashboard can use that to collate an aggregated pool of permissions based on the publicly available terms and conditions of each data collector. The DPA can facilitate this process by mandating that certain categories of information must be disclosed by all data collectors in the public domain so as to enable a third party dashboard to collate the necessary information.

Alternatively, in case the DPA proposes to mandate the provision of such a dashboard service (instead of leaving it up to market based mechanisms) it will become necessary to assess the trustworthiness and incentives of the dashboard operator, similar to the case of data trust scores. This may require some form of supervision of such entities by the DPA or some other body.

PURPOSE SPECIFICATION AND USE LIMITATION

Purpose Limitation

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

We think that the purpose specification and use limitation principles are extremely important, and have to form an integral part of the data protection law.

There exists an information asymmetry in the current market, between the data controllers (such as Facebook and Google) and consumers. The increasing interest in personal information in the industry is accompanied by an increasing under-estimation by consumers about the value of their personal data and ignorance about the scale and precision of data collection and its associated uses. The fact that data, almost inevitably, involves secondary use for purposes not originally envisioned and involves multiple participants (for collection, storage, aggregation, analytics, and sale), increases the information asymmetry and reduces the control that individuals have over their own data. In this context, it becomes extremely important to ground the data protection law with principles of purpose specification and use limitation.

A good example of why purpose specification and use limitation is important is that of the popular photo-sharing app Snapchat, where photos are said to disappear or self-destruct in a couple of seconds after they are sent and received. However, subsequent features on the app, such as “Snapchat Stories” or “Our Story” or “Snapchat Discover” now retain the pictures from up to 24 hours to a couple of days. Thus, informing users of each change in purpose, becomes necessary, especially if in the future, Snapchat started retaining the data in its archives in a permanent form, thus changing the very basis on which the app was founded and popularised. Purpose limitation thus prevents companies from creating a vast user base by setting out privacy-friendly policies, and then changing the purpose or use of the data collected dramatically, and relying on the inertia of users to continue using their app/service/products

Finally, both purpose and use limitation must be preceded by the principles of collection limitation and data minimisation - which require that (a) there must be a legal basis to data collection (and not unfettered collection) and (b) that only that data is collected which is reasonably necessary for the purpose to be fulfilled. First, unregulated collection of data dramatically increases the risk of breach. If unlimited quantities of data are gathered and stored — even if they are never analysed or applied to any uses — the risk of a single breach grows with each new wave of data scooped up or shared. The frequency and fallout of data breaches becomes more apparent each day, from Aadhaar in India to Equifax in the U.S. Second, unregulated data collection opens up new modes of surveillance, both government and corporate, that can have an extreme chilling effect on online freedoms. In the ***Digital Rights***

Ireland (2014) decision of the European Court of Justice, the courts noted that the mere collection of metadata that could identify individuals or reveal insights about them was problematic. It "*is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance,*" the courts said. Hence, a strong collection limitation and data minimisation rule must be incorporated in the law.

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

We find that the White Paper does not give enough guidance regarding the manner in which purpose specification and use limitation principles *should* be modified in the age of big data, except to state that "*In light of recent developments in data flow practices and new technologies, data may be multi-functional and being required to specify each use in an exact manner within a privacy notice may prove to be burdensome*".

We are of the view that merely because informing the data subject about new uses of their personal data (beyond what they had originally consented for) is "burdensome", does not absolve data controllers of their responsibility to specify the use of the third party personal data. This is especially considering the recent stand of the Supreme Court of India in ***Puttaswamy v UOI*, (2017) 10 SCC 1**, which affirmed the fundamental nature of the right to privacy and informational self-determination.

One option could thus be to require data controllers to get the subsequent consent of the data subjects for each specification of a new purpose, with such a term possibly being defined in the law.

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?

The reasonableness standard is envisaged by the White Paper as permitting a subsequent use of data as long as an individual could have reasonably expected such use at the time of collection and consent. However, instead of such a standard, it may be useful to apply the reasonableness standard in assessing the compatibility of the subsequent use of data, in comparison with the original stated purpose. Thus, the subsequent use of data that is collected for providing you health insurance, may not be reasonable if it is then used for assessing your application for a housing loan. However, the determination in each case would depend on the nature of the data, the original purpose of collection, and its revised use. We propose that such a determination may either be made by the DPRA in response to individual complaints or by the DPA in the exercise of its supervision and monitoring functions.

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

We agree with the White Paper's views that "*standards may have to be developed to provide guidance to data controllers about the meaning of data minimisation in the context of their data collection and use*", since principles of data minimisation have to inform the collection, storage, and use of personal data.

In areas where there are sectoral regulators, we feel that useful synergies can be achieved through coordination between the sectoral regulators and DPA. Therefore, instead of having specific demarcation of responsibilities between the DPA and sectoral regulators, the law should mandate the creation of cooperation mechanisms between them. This comment is applicable not just to standard relating to purpose limitation but on all other aspects of data protection that will be covered under the new law.

Some guidance in this context can be drawn from the recommendations of the Financial Sector Legislative Reforms Commission (FSLRC) relating to the cooperation between financial sector regulators and the Competition Commission of India. The following elements were suggested in this regard:

1. Consultation for draft regulations - The CCI should review draft regulations issued by the regulator for public comments and provide its inputs on the potential competition implications, if any. The regulator must consider the representation made by CCI before finalising the regulations.
2. Review of regulatory provisions - CCI must be empowered to monitor the effects on competition of any regulatory actions and practices on an ongoing basis.
3. Reference by CCI and regulators - Both the CCI and the regulator must make a reference to the other agency while initiating any proceedings that could potentially fall under the domain of the other agency.
4. Memorandum of understanding - CCI and the regulator to enter into a memorandum of understanding to establish the procedures for co-operation between them, which may be modified by them from time to time.

We recommend that the data protection law should provide for similar mechanisms for governing the interaction between the DPA and the sectoral regulators. This would include consultation on framing of regulations applicable to entities in a particular sector; making a reference to the other agency while initiating supervisory actions against a regulated entity and requirement to enter into a MoU to mutually agree on the procedures of cooperation between them.

This interaction becomes especially important in light of the fact that it may take some time for the DPA to build a body of regulations that would be applicable to different categories of stakeholders in different contexts. Till such time that the DPA formulates the relevant standards, the sectoral regulators would be well placed to frame appropriate standards for their regulated entities based on the principles laid down in this law. Going forward, once certain baseline standards are put in place by the DPA, these may still be supplemented by additional standards set by various sectoral regulators. The DPA and the sector regulator may also act jointly, under the terms of the proposed MoU, to arrive at the appropriate standards for a particular sector.

Such a mechanism will ensure that there will be a minimum baseline data protection available to every individual, with certain sectors such as the financial sector or the health sector, imposing additional burdens given the sensitive nature of the personal information involved.

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

Apart from the focus on purpose specification and use limitation, it is very important to also think about "collection limitation" principles. Although the White Paper references the privacy principle of collection limitation, it does not find any reference as part of the questions or components of the data protection law. Collection limitation is as important as purpose specification, since it sets the standard for determining, whether, for instance, in the context of Aadhaar, the collection of DNA profiles of individuals, as part of their core biometric information, would amount to a violation of this privacy principle.

STORAGE LIMITATION AND DATA QUALITY

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

We believe that storage limitation and data quality are very important principles. We agree with the Committee's provisional views, insofar as they state that storage of data should be done as is reasonably necessary, and such a standard will be interpreted by the industry, the DPA, the DPRA, and the courts in different contexts.

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

In case it is the individual who is providing the data, the onus should be on the individual. However, the storage and processing of the data is at the stage of the data controller, and therefore they have an obligation to ensure the accuracy of the data, especially given their secondary use of the data. One possible way of ensuring this is by providing the user with a continuous update of her data and the chance of correcting it if there are mistakes.

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

If data is properly anonymised, allowing it to be retained in this form may have some benefits over complete erasure. However, the advent of big data analytics has also revealed that even anonymised data may not be entirely secure, and the identity of the information or the content of the data may be revealed, especially when the data is used in conjunction with other available datasets. Given this challenge, we find that the White Paper has not made it entirely clear why anonymisation of data is preferable to complete erasure. We therefore need a further debate on the merits and demerits of these two options, particularly given that our current laws - whether the Aadhaar Act or the IT Act - only speak about complete erasure.

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

The law should also factor in those situations, where the data subject may withdraw consent to the collection/use/storage of data, and thus, the data may have to be deleted on their request.

INDIVIDUAL PARTICIPATION RIGHTS - 1

What are your views in relation to the above?
We agree with the Committee that individual participation rights, lie at the heart of data protection legislation and "*allow an individual to participate in, and influence the manner in*

which, their personal data is used by data controllers and other individuals". While cost and technical challenges may be a concern, it cannot come in the way of enforcing these rights.

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

We do not think that there should be any categories of information, whose access should be restricted or denied to the concerned data subject. For example, the proviso to section 28(5) of the Aadhaar Act precludes an Aadhaar number holder from accessing or correcting their core biometric information, without really explaining why such a prohibition is in place. Such restrictions should not be included in the data protection law.

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?

The right to rectification should extend to getting inaccurate data rectified. At this stage, there is no need to extend the rectification right to a right to destroy inaccurate data, but it is important to reiterate that all data should be subject to a reasonable storage limitation, as discussed above.

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.

A reasonable fee could be imposed to exercise the right to access and rectify one's personal data, which should be regulated by the data protection authority/sectoral regulators. The fee should be a reasonably low amount, so that it does not serve as a measure of exclusion of the poor. The fees should balance the need of accessibility by everyone against tenuous requests that may be made. It may be useful in this context to analyse the costs and benefits of the low fees that are charged under the RTI Act, and the effect it has had on improving transparency vis-a-vis promoting tenuous requests.

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

Yes, there should be a fixed time period within which organisations must respond to the requests by data subjects, say 30 or 45 days. It is important to note, however, that technology and APIs may change the time taken to respond to such requests. The time limits or response mechanisms being prescribed in the law should therefore take account of the available and evolving technologies so as to avoid specifying too lenient a framework.

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?

The White Paper has not adequately delved into the issue of automated decisions, what alternatives could be used, and what remedies it has in mind, nor has it discussed the UK experience, where the logic behind the automated decision has to be communicated to the data subject.

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.]

The exceptions to the right to access/correct/rectify data could include a reasonable belief that access would pose a serious threat to the life, health or safety of any individual; or to public health or public safety; or that such access would have an unreasonable impact on the privacy of other, amongst others; or if compliance is impossible. However, these decisions should be open to questioning and challenge.

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

We have already outlined our views above on the role and functions of the DPA and DPRA, which may be considered here.

INDIVIDUAL PARTICIPATION RIGHTS - 3: RIGHT TO BE FORGOTTEN

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

We are of the view that any inclusion of the right to be forgotten has to be carefully considered, especially given its impact on the right to freedom of speech and expression. Of primary importance in this debate is agreement about the definition of "right to be

forgotten", and whether it includes a right to complete erasure of public documentation or information (such as an old newspaper article about yourself), or it is a right to be de-indexed from popular search engines or whether it is limited to removing personally identifiable information (such as details of your address or phone number that are available on the internet).

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

At the very least, the right to be forgotten should be restricted to personal data that Individuals have given about themselves, in that, it should not extend to third party information (such as a news report) about individuals. However, once again, without a larger debate about the value of including the right to be forgotten within the individual participation rights, especially given the impact on freedom of speech, it should not be assumed to a prerequisite to privacy right.

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

Yes it does, inasmuch as it allows a right to erasure, but it is not clear that such an additional protection achieves an overall good, in the larger context of free speech and information. It is relevant to note here that the right of the public to receive information is also an important facet of Article 19(1)(a) of the Constitution.

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

As understood in other countries, the right to be forgotten would entail such a prohibition (e.g. the *Google Spain* case), but in the Indian context, it would depend on how the right is defined.

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?

If a right to be forgotten is adopted in the law, then in the first instance it would be the obligation of the data controller to apply the balancing principles set out in the law or

framed by the DPA against the data subject's rights. However, in the event that the individual still disagrees with the determination made by the controller a claim would lie before the proposed DPRA, which will then need to perform the balancing exercise based on the facts of the case and the principles set out in the law.

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)?

We are of the view that it would be incorrect to conceive of the right to freedom of speech and expression as an "exemption" to this right, since this is a fundamental right guaranteed under Article 19(1)(a). If the Legislature does decide to include a right to be forgotten, it would have to justify the reasonableness of the restrictions on the ground of Article 19(2), i.e. being in the interest of "sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence."

Are there any alternative views on this?

It is important to note that the Supreme Court's views on the right to be forgotten in ***Puttaswamy***, were in the nature of an *obiter* (apart from not being a view of the majority), and a subsequent Court may take a different decision. Even the Karnataka High Court in ***Sri Vasunathan v. The Registrar General*** made only a passing reference to the right to be forgotten and did not determine the question per se. Further, this question is also pending before the Delhi High Court in ***Laksh Vir Singh Yadav v. UOI***.

PART III - REGULATION AND ENFORCEMENT

ENFORCEMENT MODELS

What are your views on the above described models of enforcement?
Does co-regulation seem an appropriate approach for a data protection enforcement mechanism in India?
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?

Are there any alternative views to this?

The Committee posits the co-regulatory approach as an ideal middle ground between self-regulation and 'command and control' approaches. However, we think that a strong codified primary legislation, followed by secondary legislation by the DPA/ sectoral regulators, accompanied by a robust and open consultation process is an appropriate model. As explained below, we refer to this approach as a "consultative command and control model", which shares many common elements with co-regulation but within a robust regulatory framework.

Co-regulation is an attractive regulatory approach but its benefits compared to a consultative command-and-control method may be overstated. For the model of coregulation to be an effective check on regulated entities it still requires:

(1) Self regulatory codes to be endorsed by the DPA
(2) Self-regulatory codes to be accompanied by a credible legal threat if there is non-compliance.
(3) In order to assess compliance with these code, the DPA will have to undertake intensive monitoring and reporting.

Thus, it does not significantly reduce the burden on the regulator as compared to 'command and control' approaches and therefore, this benefit should not be overstated. Moreover, in an evolving and technical field like data protection, industry input will be invaluable but it will also need to be closely scrutinised for bias. Such bias can be best brought out through a rigorous and open consultative process for the formulation of rules and guidelines by the DPA and sectoral regulators.

The final decision making power to make regulations should vest in the DPA, which will also be responsible for monitoring and compliance. In addition, having provisions of reporting to the DPA at periodic intervals is a way which inculcates these values in the data controller's activities will also facilitate the efficient discharge of its functions by the DPA.

Having said that, we also note that the data protection law will apply to a number of data processors in varying contexts and with different levels of risk. It would not be reasonable to expect that the DPA would be in a position to immediately frame appropriate regulations on all relevant aspects. A self regulatory approach that operates within the framework of the key principles set by the law would therefore be most appropriate in the following circumstances:

a) For all data collectors till such time that appropriate regulations are framed by the DPA or sectoral regulators for a particular context; and
b) In areas where the DPA or the sectoral regulator does not find it appropriate to lay specific details through regulations.

ENFORCEMENT TOOLS

Codes of practice

What are your views on this?

What are the subject matters for which codes of practice or conduct may be prepared? 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?

Who should issue such codes of conduct or practice?

How should such codes of conduct or practice be enforced?

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

Are there any alternative views?

Codes of conduct are an important way in which to translate general principles into specific enforceable rules attuned to particular contexts. In India we often find regulators using a variety of instruments such as guidelines, directives, press releases, regulations, etc., in addition to which there is a system of rules being framed by the government. We recommend that any code of conduct issued by the DPA or the regulators should be in the form of regulations and should go through the process of regulation-making. Accordingly, such codes of conduct would be binding on regulated entities and enforceable as law, no different from other secondary legislation. The specific consequences of their violation will be decided according to the context.

As explained above, the codes of conduct should be formulated by the DPA or sectoral regulators after following the proposed regulation making framework, which includes an open consultative process. The European example of industry providing templates for the supervisory authority to approve, which has been discussed in the White Paper, might be one of the starting points for the initiation of this process. Alternatively, it could also emerge as an input submitted by the industry to the regulator in the course of the consultation process. In either case, the regulation making process should allow various interest groups to put forth their recommendations on the proposed code of conduct and the regulatory authority may incorporate these as it sees fit, with appropriate justifications for the same.

Personal data breach notification

What are your views in relation to the above?

How should a personal data breach be defined?

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

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

What details should an breach notification addressed to an individual contain?

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

We are broadly in agreement with the provisional views put forth by the Committee regarding the obligation to notify data breaches to the concerned individuals and the DPA. A personal data breach would include any unauthorised access, disclosure, alteration or loss of an individual's personal data. Any failure or attack on the pseudonymisation or anonymization techniques used by the data collector should also be treated as a breach. The notification requirements would apply irrespective of whether the breach is caused by a source within the data collector's organisation or an external source or whether any resulting harm is identified to have been caused due to it.

The primary law should contain the obligation to notify individuals and the DPA of the breach, the broad heads of the type of information that needs to be disclosed, which may be different for notifications issued to the customer and the DPA. The time period within which the information needs to be disclosed may also vary depending on the type of breach and the nature of information that has to be compromised. For instance, the breach of financial information which can be used for committing fraudulent transactions needs to be notified to the individual on a more immediate basis compared to certain other types of information. We recommend that the law should specify the broad principle of serving the breach notice in an expeditious manner with a maximum period. Within this range the DPA or sectoral regulators, where applicable, may specify shorter time limits for different contexts.

DATA PROTECTION AUTHORITY

What are your views on the above?
Is a separate, independent data protection authority required to ensure compliance with data protection laws in India?
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?

We propose the establishment of two new agencies under the data protection law:
(i) a Data Protection Authority (DPA) that will function as a cross-sectoral privacy regulator, which exercises legislative powers (drafting regulations that are binding on regulated entities), executive (in its supervision and monitoring activities) and quasi-judicial functions (assessing compliance with the law by regulated entities and initiating enforcement actions): and
(ii) A Data Protection Redress Authority (DPRA) that will be responsible for adjudicating individual complaints and affording appropriate remedies to individuals.

Rationale for separate agencies

A similar division of responsibilities between regulatory and supervisory powers and the redress function was recommended by the Financial Sector Legislative Reforms Commission (FSLRC) in the context of the financial regulatory architecture. One of the key objectives of this design is to allow the regulator as well as the redress agencies to focus exclusively on their core functions. This becomes particularly important in the present context, given the principles based nature of the proposed law. In such a scenario, the DPA will be tasked with the responsibility of formulating appropriate regulations on different aspects of data protection and for different contexts and conducting supervision activities to ensure compliance with the law.

Given the large number of data collectors in the system and the individuals interacting with them, it would be unrealistic to expect the DPA to also take up the responsibility of investigating individual complaints. The most pervasive challenge across data protection authorities globally are that they are understaffed and lack resources to address a mandate that includes both private and public sector. In this background, even the most well staffed DPAs (such as those in Germany and Netherlands) are extremely selective with the enforcement actions they pursue – usually managing only three-four major investigations each. Audits and notification requirements have been the primary investigatory and enforcement tools of DPAs, and here too DPAs struggle to incorporate a technical audit beyond merely an audit of policies and paper trails. Thus, the ability to act on individual user complaints acts as an additional constraint on the DPA's human resources.

In general, annual reports of DPAs in other jurisdictions indicate a low number of complaints being filed by individuals. This could be attributed to the fact that there is generally no promise of compensation from the DPA, and moreover, the information deficit when it comes to privacy harms means that user is not always well placed to identify breaches. In May 2018, the GDPR will become effective in Europe. This is touted to increase consumer awareness of data breaches and increase the prevalence of complaints by individuals and groups. We can expect a similar trend in India also, pursuant to the enactment of the data protection law. Accordingly, we propose the need for the creation of a separate DPRA that will be exclusively tasked with the function of providing redress for individual complaints and awarding compensation for the same.

Another important reason to separate the functions of regulation and redress stems from need to avoid any conflict of interest that may arise from making the same agency responsible for the framing of regulations and providing redress for their breach. A large number of complaints on a particular issue not only reflects that data collectors have not been acting in compliance with their requirements but also that the regulator (in this case DPA) may have failed to take appropriate regulatory or supervisory actions to curb such malpractices. It is therefore important that the resolution of any complaints should take place independent of the other core

functions of the regulator. There should however be a strong feedback loop between the DPRA and the DPA using which the DPA can gain information about the type of complaints being raised, the entities to which they relate and the underlying causes. This will enable the DPA to address such issues through appropriate amendments to it's regulations or by initiating enforcement actions against particular data controllers.

Design and functions

Drawing once again from the detailed recommendations made by the FSLRC on the design of regulatory agencies, we propose that the following elements should be incorporated in the design and functioning of the DPA:

(i) *Separation of powers within the organisation*: The three functions of the DPA, as noted above, need to be clearly delineated and a separation of powers between the officers in each wing needs to be maintained to ensure independent functioning. Therefore, persons involved in enforcement functions should not be involved in the framing of regulations and vice versa. This is particularly important since the DPA will enforce provisions against both public and private bodies.

(ii) *Transparent regulation-making processes*: The law should mandate the DPA to ensure transparency in the discharge of all its functions. In particular, it should specify processes for effective public participation in the regulation-making processes. This will ensure a system of checks and balances while also helping to improve the information and analysis of the DPA. Further, the DPA should also undertake an assessment of the expected costs and benefits of the proposed regulation and seek to adopt measures that minimise the compliance costs while meeting the intended objective. Finally, the law should also mandate the DPA to provide an explanation for the decision finally adopted by it and the broad reasons for acceptance or rejection of the comments raised by stakeholders and the public.

(iii) *Executive and quasi-judicial functions*: The law should also specify transparency and due process requirements in respect of the discharge of the other supervisory and regulatory functions of the DPA. This would include requirements such as completion of investigations with a specified time frame, efficient processes for registration of various entities and collection of information from them and adherence to the rule of law while carrying out enforcement actions.

(iv) *Judicial review mechanism*: A clear judicial process should be available to persons who seek to challenge the actions of the DPA. For this purpose we support the need for designating an appellate tribunal to hear appeals against the DPA's orders. This could be done by conferring this power on any of the existing tribunals or creating a new forum for this purpose. In either case it would need to be ensured that the tribunal is staffed with judicial officers who have

appropriate qualifications and experience in law and technical expertise in the field of data protection and data science.

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

The DPA should consist of a Chairperson and a team of executive and non-executive members. The Chair, along with the executive members, would be responsible for the day-to-day management of the DPA. The non-executive members will consist of experts in the fields relevant to the operations of the DPA who will be appointed on a part-time basis. As suggested by the FSLRC in the context of financial regulators, one of the executive members of the DPA should be an administrative law member who will be in charge of the team responsible for undertaking enforcement actions in the DPA. This will enable a logical separation between the regulation-making, executive and enforcement actions within the DPA.

Further, the process for selecting the members of the DPA should operate in a fair and transparent manner. Drawing again from the recommendations of FSLRC, we propose the need for a professional search and selection committee in order to ensure that the selected members are competent persons with relevant knowledge and experience. For this purpose, the government should maintain a panel of experts from relevant fields such as privacy, technology, data science, law, economics, etc who can serve as members of the selection committee. Further, independence from the government should be ensured by requiring that the majority of the members must be persons who are not related to the government.

The integrity of the selection procedure will be protected by requiring that all short-listing and decision making are done in a transparent manner. For this purpose, the committee should disclose all the relevant documents considered by it and prepare a report after the completion of the selection procedure. This will include the minutes of the discussion for nominating names, the criteria and process of selection and the reasons why specific persons were selected. Further details in this regard are available in the report of the FSLRC and the draft Indian Financial Code drafted by them.

Considering that a single, centralised data protection authority may soon be over-burdened 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?

In the model suggested above, the DPA will not be handling individual level complaints and therefore it may not be necessary for it to establish regional offices in the immediate future although the law should make provisions for the same. Depending on the volume of work generated by it, the DPA may subsequently find it useful to set up such regional offices to assist it in the discharge of its supervisory functions.

The DPRA, on the other hand, would find it useful to set up front-end offices and facilitation centers throughout the country from the very beginning. Individuals residing in rural as well as urban areas should be able to access these officers in order to gain awareness about the data protection framework and submit their complaints. As suggested by FSLRC in respect of the proposed Financial Redress Agency, modern technology should be used to connect these front-ends into a centralised mediation and adjudication system maintained by the FPRA.

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

The independence of the members of the DPA can be ensured by building in appropriate systems in the law regarding the terms of appointment of members, their tenure and grounds for removal. Drawing from the recommendations of FSLRC we propose that the members should have a fixed term of (say) five years, subject to a retirement age for executive members. The members (but not the Chairperson) may be reappointed for another term subject to going through a fresh process of nomination by the selection committee process. This will ensure that the tenure of members should not extended as matter of course, which contributes to ensuring independence in the discharge of their functions.

The salaries and other entitlements of the members would be fixed by the Government, however once fixed, they should not be varied to the detriment of the members. Further, the law should clearly specify the reasons for which a member may be removed and the process by which removal may take place.

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

Any penalties/ fines recovered by the DPA should be transferred to the Consolidated Fund of India. In the event that he DPA is allowed to retain a portion of the fines it could create perverse incentives to levy higher penalties.

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

Please see responses to the above points and the questions in the Adjudication section.

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?

We propose the need for formal coordination mechanisms between the DPA and sectoral regulators. Please refer to our comments in the the section on setting of standards for purpose specification and use limitation for detailed recommendations in this regard.

Besides this, we also propose that the law should empower the DPA to appoint various committees as may be necessary to assist it in the discharge of its functions. It would be particularly useful to put in place a multi-stakeholder committee that can advise the DPA on the framing of standards that may be applicable in different contexts and the interpretation of the data protection principles laid down in the law. The creation of a similar multi-stakeholder committee mechanism has been suggested by researchers in the context of the Aadhaar Act to facilitate a balance between the privacy of individuals and the need for more open data in the Aadhaar ecosystem.[4]

The "Article 29 Working Party" in the European Union could also be a useful example for incorporating such a mechanism in the Indian data protection law. This Data Protection Working Party was established by Article 29 of Directive 95/46/EC, consisting of representatives of national supervisory authorities, European Data Protection Supervisors and a representative of the European Commission. The role of the Working Group is to provide the European Commission with independent advice on data protection matters and helps in the development of harmonised policies for data protection in the EU Member States.

ADJUDICATION

What are your views in relation to an adjudication process envisaged under a data protection law in India?
Should the data protection authority have the power to hear and adjudicate complaints from individuals whose data protection rights have been violated?

[4] Vinod Kotwal, Smriti Parsheera, Amba Kak, Open data & digital identity: Lessons for Aadhaar, ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K), 2017, available at http://ieeexplore.ieee.org/document/8246983/.

As the White Paper's provisional views point out, a mechanism for stringent penalties as well as direct compensation to individuals are critical to ensuring effective implementation of the data protection law. We agree that the DPA should be empowered to impose significant penalties and burden on regulated entities through the exercise of its monitoring and enforcement powers. However, as noted above, we propose that the adjudication of individual complaints should be handled by a separate agency, the DPRA. We propose the following steps in this regard:

(i) In the event of a complaint emanating from a violation of the data protection law of the regulations framed by DPA, the individual would first be required to make a complaint to the concerned entity. The law should require all data collectors and processors to put in place appropriate mechanisms for dealing with any such complaints, which may be supplemented by further details specified by the DPA through regulations. In the event that a complaint is not resolved to the satisfaction of the individual, she may file a complaint with the DPRA.

(ii) The DPRA will consist of a team of qualified mediators and adjudicators. In the first instance, the DPRA will attempt to facilitate an amicable settlement between the individual and the data collector through a process of mediation process. In cases where the parties fail to reach a settlement the DPRA would proceed to decide the case through adjudication.

(iii) The adjudication order issued by the DPRA may provide for an award of compensation to the individual or order the data collector to refrain from acting in a particular manner. Any party that is dissatisfied by an adjudication order made by the DPRA may bring an appeal before the designated tribunal.

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?
Should appeals from a decision of the adjudicating officer lie with an existing appellate forum, such as, the Appellate Tribunal (TDSAT) ?
If not the Appellate Tribunal, then what should be the constitution of the appellate authority?

Appeals from the decision of the DPRA should lie with a designated tribunal which should be the same as the tribunal that will be entitled to hear cases in respect of any actions taken by the DPA. This role could be cast on any of the existing tribunals, subject to ensuring that the tribunal has adequate capacity and system to effectively discharge these functions, or a new tribunal may be created for this purpose. Please refer to the recommendations of the FSLRC regarding the design and functioning of a proposed Financial Sector Appellate Tribunal, many of which are also relevant in the context of the data protection tribunal.

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

An effective redress body needs to be designed in a manner that ensures access, convenience, efficiency and speedy remedies. In the context of redress of complaints arising in the financial sector, the FSLRC had recommended that the redress agency must function as a technologically modern organisation that will carry out video hearings, digital handling of documents, telephonic/online registration of complaints, maintenance of a high quality electronic database and online tracking of compensation payments.

Similarly, the data protection law should require the DPRA to put in place adequate systems, processes, technology and infrastructure to enable it to efficiently discharge its functions. Further guidance on issues relating to the proposed design, functions, human resource and other requirements of the DPRA can be drawn from the report of the Task Force on the Financial Redress Agency that was set up by the Ministry of Finance.[5]

Should the data protection authority be given the power to grant compensation to an individual?
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?
Can an appeal from an order of the data protection authority granting compensation lie with the National Consumer Disputes Redressal Commission?
Should any claim for compensation lie with the district commissions and/or the state commissions set under the COPRA at any stage?

As per the proposed framework this power of granting compensation to individuals would vest in the DPRA and not the DPA. The ability of the DPRA to grant compensation up to a certain cap is essential to strengthening its role as a redress agency. Absent such a provision, the requirement to approach civil courts to obtain compensation would add an additional disincentive for aggrieved person to approach the DPRA.

Experience from other jurisdictions shows that obtaining compensation for **non-monetary damages** can also be a major impediment to consumer empowerment**,** as seen particularly in case of class action suits in Europe. The UK case of ***Google* v. *Vidaal Haalt*** is instructive as the Court concluded that, given that the aim of the data protection law is to protect privacy, it would be odd to prevent a claim by data subjects whose privacy was breached but who had suffered distress, without pecuniary loss. The GDPR in Article 82(1) resolves this issue by stating that any person who has suffered "material or non-material damage" as a result of a breach of GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The

[5] See http://dea.gov.in/sites/default/files/Report_TaskForce_FRA_26122016.pdf

inclusion of "non-material" damage means that individuals will be able to claim compensation for distress or dignity harms even where they are not able to prove financial loss.

We accordingly recommend that the DPRA should also be entitled to award compensation for financial loss as well as any loss or damage caused to an individual on account of any material distress or inconvenience due to actions taken by the data collector in breach of the law and regulations. The maximum amount that may be awarded by the DPRA as compensation should be specified in the law.

In the event that a cause of action arising under the data protection law also entitles the individual to a separate remedy under the Consumer Protection Act, the individual should be free to decide which of these option they want to pursue. In case the Government determines at a later stage that the DPRA is effectively discharging its adjudicatory functions it may take a decision to make statutory amendments to exclude the jurisdiction of consumer forums.

PENALTIES

What are your views on the above?
What are the different types of data protection violations for which a civil penalty may be prescribed?
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?
In view of the above models, how should civil penalties be determined or calculated for a data protection framework?

Given that the state is arguably the largest data collector and processor in the country, and that collection by the state is often mandatory, the DPA regime must apply with equivalent strictness to both public and private sector entities in terms of both compensation and penalties. That said, certain distinguishing factors (such as the source and extent of finances) must be taken into account. We recommend a system of imposing monetary penalties that will include distinct parameters for private and public sector entities.

The UK experience is instructive in this regard. Section 55A of the UK Data Protection Act was amended in 2010 to give the Commissioner the ability to impose a civil monetary penalty of up to 500,000 GBP on a data controller, whether a private or public body. The exact amount of penalty is determined by a number of factors, including the impact on the entity being penalised and their ability to pay. In fact, fines against public sector controllers are predominant, and

many attribute this to the highly sensitive data held by the public sector in the UK (eg. health records, prison records).[6]

The design of penalties is also important. Ultimately, the point of a penalty is to deter violations in the future. Data controllers should be given the signal that the costs of violation are higher than the benefits, despite the low probability of being caught. Deterrence is achieved not only when fines are levied, but when fines are seen to be levied. Given this, our view on the design of penalties is shaped by FSLRC recommendations namely:

- For each violation, the regulator must carry out an investigation on the illegitimate gain made by the violator;
- The regulator must make an effort to determine the amount of illegitimate gains made by the violator;
- The penalty should be a multiple of the illegitimate gain, but limited to a maximum of 3 times the illegitimate gain;
- The cause of the violation - whether it was a result of deliberate action or negligence should play a role in the determination of the penalty
- The regulator must compensate any direct victims of the violations if they can be ascertained;
- If no direct victims can be ascertained, the funds must be transferred to the Consolidated Fund of India; and
- The regulator must have regulations and processes for calculating and enforcing the fines.

We think that these principles should be a part of the primary law. The details on the exact nature and quantum of the fines should be further developed through regulations.

Apart from penalties, cooperative processes such as consensual audits, training, public guidance are all effective means of ensuring compliance with the law.

Finally, we note that each data controller must put in place appropriate codes of conduct and internal mechanisms to ensure adherence with the data protection law and regulations by its employees and agents. Where a data breach or violation can be traced to an employee of the data controller, this should attract appropriate consequences, which could include initiation of disciplinary proceedings against a public sector employee.

We also find some examples of legislations where the law allows for the attribution of liability on specific public servants in case of their failure to deliver an identified service. For instance, Section 20 of the RTI Act allows for the imposition of a penalty of Rupees two hundred and fifty per day (up to a maximum of rupees twenty-five thousand) upon a Central Public Information

[6] *See* Enforcing Privacy, ed. David Wright and Paul De Hert 2016

Officer or State Public Information Officer who refuses to meet a legitimate request for information under the RTI Act. Similar provisions are also seen in certain state legislations on delivery of public services. For instance, the Karnataka Guarantee of Services to Citizens Act, 2011 provides for a payment of compensation of Rupees twenty rupees per day (upto a maximum of five hundred rupees) for the delay in the delivery of a guaranteed service. This amount can be recovered from the designated officer who was responsible for the provision of such service.

On one hand, such mechanisms may be considered to be a means for enhancing accountability of individual officers in particular contexts. On the other, they lead to concerns about staticity in policy actions and difficulties in the attribution of liability, particularly in contexts such as a data protection framework where it would be difficult to identify specific individuals who may be responsible for actions that lead to enforcement actions or specific claims under the law. We would therefore caution against the use of such mechanisms under the data protection law.