To,

THE COMMITTEE OF EXPERTS ON DATA PROTECTION FRAMEWORK FOR INDIA

C/o
Shri Rakesh Maheshwari
Scientist G & Group Co-ordinator, Cyber laws
Ministry of Electronics and Information Technology (MeitY),
Electronics Niketan, 6, CGO Complex, Lodhi Road,
New Delhi- 110003.

Subject: Comments on the White Paper published by the Committee

Please find appended below a note with my comments on the White Paper. Please note that the views expressed are personal, and do not reflect the position of the National Institute of Public Finance and Policy.

Sincerely,
Suyash Rai

Senior Consultant
National Institute of Public Finance and Policy,

18/2 Satsang Vihar Marg,
Special Institutional Area,
New Delhi 110067.
[Near JNU East Gate]

Mobile: 8285475779

Comments on the White Paper of the Committee of Experts on a Data Protection Framework for India

I congratulate the Committee for bringing out a comprehensive White Paper, covering a wide range of issues and a variety of perspectives. It serves as a good starting point for public discussions on regulation of data protection.

The law itself will not ensure data protection. It is more important to ensure that the law is implemented through an effective regulatory system. The overall theme of my comments is that there is a need to be pragmatic while making the data protection law, i.e. any proposed legislative framework should be judged on the basis of its practical consequences. This is simply because ultimately we care about outcomes and not just expression of good intent. In India, we have had many ambitious laws that did not lead to expected outcomes. The implementation of a law depends on a variety of context-specific factors, such as regulatory capacity, resource availability, scale of a country, adjudication system, and so on. So, the same law may have very different practical consequences in India, than it would have in, say, UK. Pragmatism demands careful thinking about the nature of the problem and the context in which it is to be addressed. The law should be such that it ensures good outcomes in the long run, even if it disappoints some activists in the short run. In this note, I have largely focused on strategic issues in framing a data protection law in India.

The note begins with some observations and analysis around: challenges of regulatory capacity; the economics of data protection regulation; the rights-based approach to regulation; issues of jurisdiction; the need to distinguish between data protection and broader privacy concerns; challenges of enforcement against government organisations; and the need for enabling "safe" innovations. In my view, proper reflection on these issues will help create an effective law for data protection. At the end of the note, some specific suggestions on the legislative formulation are given. These suggestions flow from the analysis.

1) Limitations of regulatory capacity, and how the law may shape regulatory capacity:

The success of this law, like any regulatory law, would largely depend on its implementation by the regulatory authority established to make regulations, monitor compliance, take enforcement actions and give redress. On regulatory capacity, I would like to make three India-specific points that are worth considering while proposing a new data protection law: first, the capacity in regulatory organisations is much weaker than that in countries presently implementing advanced data protection laws; second, it is almost impossible to quickly build substantial capacity in a new regulatory organisation, especially for data protection regulation; third, the mismatch between capacity and expectations can create poor outcomes, such that giving a broad mandate to a newly established data protection authority may produce worse outcomes than giving it a narrow mandate.

Relatively low regulatory capacity in India: the following chart shows percentile ranks (0 – lowest; 100 - highest) on "regulatory quality"[1] for India and the countries from where ideas are most

[1] This ranking is from the measure of the World Governance Indicators (WGI) published by the World Bank. WGI is a research dataset summarizing the views on the quality of governance provided by a large number of enterprise,

commonly cited in the White Paper. India ranks much lower than other countries, and almost all the countries cited in the White Paper are close to the top rank. Overall, in 2016, India ranked 123rd among 209 countries and territories. Generally, on most indices of state capacity India ranks close to the median. Such rankings and indices should not be treated as precise, scientific measurements of capacity, but they are useful indicators of relative capacity.

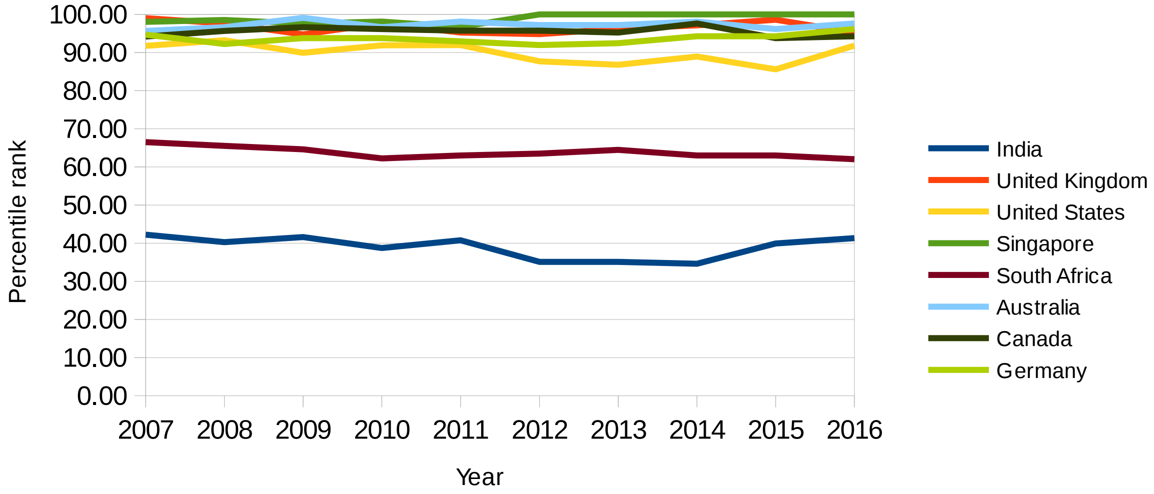

Fig 1: Percentile rank on Regulatory Quality (Source: World Governance Indicators, World Bank)

Difficulty of building regulatory capacity, especially in a Data Protection Authority: The factors that determine capacity in government organisations may include: organisation design and management; political system design; basis of legitimisation; and cultural and structural factors[2]. Most of these factors cannot be significantly altered over short periods of time, and more importantly, many of them emerge from contingent social and political processes. While it is easier to build high performance regulators in countries where government has high capacity overall, this is more difficult in India. A new regulatory organisation in India will find it very difficult to build high capacity in a short span of time.

This is particularly true of data protection regulation, because of the nature of the activities involved in such regulation. Data Protection Regulation is highly discretionary (i.e. decisions will be made on the basis of information that is important but inherently imperfectly specified and incomplete), and transaction-intensive (i.e. requires a large number of regulatory and supervisory decisions)[3]. The level of discretion may vary from one activity to another. Let me give a few examples:

- "Data breach" is a kind of violation that may require relatively less discretion to assess, as there is a limited space for disagreement on whether there was a breach, albeit when it comes to

citizen and expert survey respondents in industrial and developing countries. These data are gathered from a number of survey institutes, think tanks, non-governmental organizations, international organizations, and private sector firms. For "regulatory quality" in India, data from the following sources has been used: Bertelsmann Transformation Index; Economist Intelligence Unit; Global Insight Business Conditions and Risk Indicators; Heritage Foundation Index of Economic Freedom; IFAD Rural Sector Performance Assessments; Institute for Management and Development World Competitiveness; Institutional Profiles Database; Political Risk Services International Country Risk Guide; World Economic Forum Global Competitivness Report; World Justice Project.

[2] Fukuyama, Francis. *State building: Governance and world order in the 21st century*. Profile Books, 2017.

[3] Pritchett, Lant and Michael Woolcock (2004). *Solutions when the Solution is the Problem: Arraying the Disarray in Development.* World Development 32(2): 191-212

enforcement, there can be differences about culpability on account of negligence, etc. However, the same problem can require more discretion if "preventive" actions are to be specified to avoid breaches, as experts can disagree on the best ways to manage the risk of data breach.

- Regulating to ensure "informed consent" can require a considerable amount of discretion, because, to be implemented effectively, it will require somewhat complex assessments about whether the consent was truly informed and meaningful, or done in name only. It may be simpler and less discretionary to assess whether there was *any* consent at all, but this is far less useful for achieving good data protection outcomes.

- "Data minimisation" is one of the preventive measures that the Committee has provisionally endorsed. The core of data minimisation is that data processing should not use more data than is required for a task. This is a way in which data protection can be achieved by design. However, to actually ensure data minimisation requires regulator's staff to go into the systems of data controllers and processors, and assess which data is legitimately required for which purpose. Even if the regulator relies on self-assessment or third party audits, it will still need to evaluate these assessments and audits in a variety of contexts, ranging from financial services to healthcare. Such judgments need to be exercised with sophistication and knowledge, otherwise they will end up disrupting businesses. Take the example of wealth management in finance. A wealth manager often collects and processes a large amount of personal data. There will always be considerable discretion in assessing whether data minimisation is being achieved. The larger point here is that since mechanisms such as data minimisation are preventive, they require extensive discretion while taking sophisticated ex-ante decisions about how controllers/processors collect and use data.

Transaction intensity in data protection regulation arises out of its monitoring and enforcement functions, which will require directly or indirectly monitoring numerous *events* in a larger number of data controllers and processors across a number of sectors. The transaction intensity is also shaped by a unique type of moral hazard problem that is seen in this domain. This problem, which is discussed in more detail later in this note, arises out of the fact that "personal data" is not a finite resource to be protected. The users can, by sharing data and creating more personal data by online activities, change the scale of the problem for the data protection regulator. This ability of the users to significantly expand the work of the regulator by their voluntary actions makes data protection a unique regulatory challenge for data protection.

The combination of these two characteristics makes it more difficult to build capacity, because it is not about having a few capable individuals exercising discretion (eg. Monetary policy) or about having a large number of persons performing mechanised tasks (eg. Aadhaar enrolment; immunisation). I am not suggesting that this necessarily requires building a large, bureaucratic organisation. Over a period of time, DPA will have to develop the organisation form suited for performing these functions in India's context. However, irrespective of the form that it takes, it is advisable to be modest about expected capacity in the DPA during the initial years. Given the nature of the functions it will perform, no organisational form will help build capacity rapidly.

The mandate given to the authority may affect its ability to build functional capacity:

Given that there will be low capacity in a new data protection regulator, it is important to avoid mistakes that impede the process of building real capacity in the regulator. The most common mistake is to give a regulator a broad mandate (a combination of expansive jurisdiction and a large number of varied responsibilites) and draconian powers in its early days, when its capacity is low. The possibilities can be depicted in the following matrix[4]. Certain clarifications regarding the matrix are worth stating. First, only four possibilities are shown, even though it is obvious that there is a continuum along both variables. Second, capacity is not a static phenomenon, because it depends on the situation - some organisations perform well under stress, while others perform well during normal circumstances but collapse in situations of stress. Third, different types of capacities are required for different kinds of functions and responsibilities. To produce good outcomes, there needs to be some correspondence between capacity (the type of capacity and its performance under stress) and mandate (jurisdiction and responsibilities, and the possibilities of stress therein).

	Narrow Mandate	Broad Mandate
High Capacity	Quadrant II	Quadrant I
Low Capacity	Quadrant III	Quadrant IV

Since a new regulator will have low capacity during the initial years, the choice that the Committee has to make in its recommendation is between Quadrants III and IV. Beginning in Quadrant IV (low capacity and broad mandate) may lead to implementation failure in a number of ways:

- ***Capacity collapse under stress:*** The huge mismatch between the mandate and the capacity of the regulator, the overly optimistic expectations of the pace of improvements in outcomes, and unrealistic expectations about improvement of capacity lead to stresses and demands on systems that will affect capacity-building in the regulator[5]. The regulator may never get a chance to carefully build capacity to perform certain specific functions, because it will always remain in coping mode, in face of expectations it cannot really fulfill.

- ***Preference for form over function:*** To maintain legitimacy, the regulator may simply imitate the forms of modern institutions without actual functionality[6]. Regulators, like any government institution in a political society, needs to gain and maintain legitimacy in the society. They must do so while intermediating between a variety of conflicting interests. In face of expectations that are impossible to meet, a regulatory organisation may “mimic” forms of organisation and procedures, without functionally performing its role and producing the desired outcomes. This is a natural response when legitimacy is to achieved in a context of low capacity, great expectations and conflicting interests. The alternative is to achieve legitimacy through actual performance, but this is nearly impossible if the mandate is broad, because building capacity to deliver on such a mandate is very difficult. So, the staff of the regulator may respond by following rules and procedures but not

[4] Adapted from “Fukuyama, Francis. *State building: Governance and world order in the 21st century*. Profile Books, 2017”.

[5] See, for a discussion on this theme in a variety of contexts: Pritchett, Lant, Michael Woolcock, and Matthew Andrews. "Capability traps? The mechanisms of persistent implementation failure." (2010).

[6] Ibid.

truly concern themselves with the outcomes. This “mimicry as reform” does not yield actual outcomes. At best, it only creates a perception of performance.

- ***Misuse of powers:*** a regulator with a broad mandate is usually also given draconian powers. The legislative intent is to use the powers judiciously in public interest. However, as the organisation starts deriving more of its legitimacy by form and posturing, rather than by actual performance in delivering outcomes, this decline in integrity may also lead to inefficient and/or unfair use of powers. For instance, when faced with violations, it may be tempted to deploy a heavy-handed approach, using outright bans and disproportionate penalties, just to get legitimacy in the eyes of the public. To some extent, this problem can be overcome by placing “due process” requirements on the regulatory authority (discussed later). However, in situations of capacity collapse and decline in integrity, these checks and balances may have limited efficacy. It is, after all, difficult to hold an organisation accountable to do the impossible.

I will be happy to point the Committee to several examples of these mistakes in India and other countries. There is a rich literature on these issues.

A regulatory organisation beginning in Quadrant IV may forever be stuck in low capacity. Worse, it may lose integrity and coherence, and end up focusing more on appearance than on performance, prefering form over function. So, moving from Quadrant IV to Quadrant I would be difficult. Further, even if the political leadership sees the problems and seeks to map expectations to actual capacity, moving from Quadrant IV to Quadrant III is not politically feasible, given the politics of *reducing* protections, especially in face of fierce activism that surrounds such issues. It is a mistake to place a new regulatory agency in Quadrant IV, i.e. hobble it with a broad mandate when it has little capacity, especially in an areas where there is so much public pressure and conflicting interests. This will almost certainly produce poor outcomes.

One way in which the regulatory laws in India seem to have responded to the problem of capacity-mandate mismatch is through vagueness of objectives given in the regulatory laws. Most of the Indian regulatory laws do not give clear objectives to regulators. In the best case, the regulators pick and choose the areas of emphasis, and build actual capacity in those areas. In the worst cases, regulators simply get busy with form over function. In most cases, important areas of regulation remain substantially unaddressed. For example, in spite of the long history of the sector, there is, arguably, weak consumer protection in banking. The law does not give a clear set of consumer protections to be upheld by the RBI. It gives the RBI enormous leeway to prioritise. This vagueness is not good for accountability of regulators.

It is better for the DPA to begin with quadrant III (with a clear and basic mandate), move to Quadrant II by building capacity to deliver on its narrow mandate, and then, move to Quadrant I. It is not necessary for the first law in India to contain most of the protections being provided all over the world (as it being proposed by the White Paper, and demanded by many activists). It is tempting to be comprehensive and ambitious in law, but such an approach places excessive burdens on the regulator that is supposed to uphold the protections given in the law. We should see this law as only the first step towards building a data protection regime in India. As the regulatory system demonstrates ability to solve problems, its mandate may be broadened.

Much of the discussion happening around this issue seems to be converging around an “all of the above” approach to defining the regulatory mandate. I urge the Committee to resist pressure to recommend a law that will place the DPA in Quadrant IV. The law should be closer to Quadrant III, and lay the foundation for an effective regulatory regime for data protection. This raises the question: what is a “narrow” regulatory mandate? In my view, narrowing of the mandate entails focusing on certain “basic” protections, being pragmatic about jurisdiction, leveraging regulatory capacity in other sectors, and focusing on ensuring protections where they are most important. Some of the analysis in this note may help identify the basis for narrowing the mandate, but much more work and discussion is required to come up with a suitable Quadrant III formulation.

2) The Economics of Data Protection Regulation

In this section, I would like to draw the Committee’s attention towards certain characteristics of data protection regulation from an economic perspective. This perspective can inform the design of a law by pointing at: how incentives may be shaped by the law; how the economics of purpose and risk may help prioritise regulatory resources; and how economic analysis may help avoid wrong regulatory choices.

A unique moral hazard problem:

What is to be protected under a data protection regime is “personal data”. This data is protected from breaches, unapproved processing, etc. However, unlike, say, money, there isn’t a finite amount of personal data to be protected. Users can share the same personal data with many data controllers. Users can also create more personal data by online activity. Each instance of sharing or creating personal data adds to the risks of data protection for the user, and thereby to the scale of the problem for the data protection regime. This ability of the users to significantly expand the very field of regulation makes data protection a unique regulatory challenge. Therefore, prudence exercised by users in sharing and creating personal data is critical for data protection, much more so than in any other field of regulation. The law should not take away the incentive of the users to be prudent in decisions that they are well-placed to take.

The data protection regime might shape the behaviour of users. If the regulatory framework puts greater responsibility on the regulator to assure protections by taking preventive measures (eg. Data minimisation) and to give quick redress based on individual grievances, users would have lesser incentive to be prudent while sharing and creating personal data. This a moral hazard problem – just because someone else is giving protection against the risks, one is likely to take more risks. On the other hand, if the regulatory approach is sharply based on user responsibility and consent, and lets users incur costs of their imprudence, we can expect more prudence from users. This does not mean that there should be no preventive measures taken by regulators. However, such measures should be applied only where they are necessary. For instance, some preventive measures may be required to maintain minimum standards of data security, because users will typically not be in a position to assess this, and harms caused by a breach may be significant.

One could argue that moral hazard is not unique to data protection regulation. In banking regulation, the State promises to make efforts to keep banks reasonably safe, and takes several preventive measures to keep this promise. This gives the depositors a certain level of comfort, which makes them less likely to assess the financial strengths of a bank before putting their money in it. This is moral hazard. However, this effect works within a limited, defined space of banking, which is comprised exclusively of licensed banks. The regulator controls entry into and exit from that space. Contrast this with, for instance, mobile applications – the moral hazard would generate behavior that will expand the scale of the problem in a manner that cannot be controlled by the regulator. In data-based applications (online or real world), it is infeasible to ensure an exclusive, licensed field of protected activities. So, users would assume that the regulator will protect them, and this may lead them to be more indiscriminate in sharing and creating personal data, thereby increasing the regulator's responsibility.

It might be tempting to point at problems of achieving informed consent and to advocate regulator-led measures of data protection that limit the role of consent and focus more on ex-ante, preventive measures monitored and enforced by the regulator, but this is a road to less prudence by users and ever-increasing responsibilities and powers for the regulator. Acknowledgment of this interplay between prudence of users and the mandate of the data protection regime should inform the nature, scope and extent of protections promised by the law. One could argue that protections ensured by the regulator allow us to participate more freely, and not giving extensive protections may create a *chilling effect*, but there can also be a good kind of chilling effect, which makes us careful about sharing and creating personal data. Achieving the good chilling effect, while avoiding the bad chilling effect is a worthy objective.

Purpose vs. Risk:

There can be disagreements on the specifics, but it is easy to see that all purposes for which personal data is shared are not equally important. For example, it can be argued that some recreational applications such as mobile games are not as important as healthcare services[7], but all of them may creat risk to data protection. If we acknowledge such distinctions, we could argue that pragmatism demands that regulatoy emphasis be given to providing greater protections for protecting personal data in more important services, where there is relatively less user discretion in sharing data. This also ties in with the importance of user responsibility. Users who freely share data with applications that are generally considered to be less important (eg. games that require a lot of personal data) should deal with the consequences of their choices. It is not a good use of limited regulatory capacity to ensure data protection in such situations. The law should recognise this gradation in the importance of services.

Another distinction that can be useful is that between personal data that creates personal benefits, and personal data whose voluntary sharing can be beneficial for the society. Personal data is, in

[7] Avid gamers, who may prefer jeopardising their health for the pleasures of gaming, may disagree.

most instances, a private good, and the person whose data is protected gets most of the benefits of the protection. In some instances, however, there are positive externalities of data sharing: a person sharing data benefits others (eg. sharing data about blood group). On the margins, regulatory resources may be better used in protecting personal data with large externalities. Economic theory suggests that where sharing personal data creates substantial societal benefits relative to personal benefits, such sharing will be in under-supply. By augmenting protections for such sharing, such activities can be encouraged.

Market failures, real problems, and effective regulation:

The primary reason for regulatory intervention in markets is to address problems created by market failures. Market failures relevant for data protection are: market power, asymmetric information, externalities. Because of opacity of operations, a user is not able to monitor how her data is being used by the controller/processor, and security of the data systems. This asymmetric information could be exploited to inflict harm on the user, to gain undue benefits, to handle data negligently, and so on. There are situations where mistakes by a controller/processor can inflict harm on many users. For example, laxity of data security may lead to breach. This is an example of negative externality, where the controller/processor does not absorb the costs of the error, while saving money by investing less in data security. In some instances, a controller/processor enjoys dominant market power, so that the latter is not in a position to influence the former's decisions or to shift to another controller/processor. The problems of market power are addressed in competition laws, and should not be included in a data protection law. If required, the Competition Act should be amended.

Market failures only create potentiality of harm. Often, there is no incentive for the controller/processor to take advantage of market failures, because other incentives are stronger. For instance, the market may reward more privacy-friendly providers, leading them to voluntarily protect data of users. So, any regulation must be in response to a clearly identified and significant *problem* arising out of a market failure. Some of the protections being envisaged do not appear to meet this test: being subject to a decision based solely on automated processing; right to object to processing for direct marketing; and the right to be forgotten. Sure, these may be nice protections to have, but the scale of the problem does not seem to warrant a regulatory intervention, especially given the capacity required to solve provide these protections. These are discussed in some more detail later in this note.

Finally, it is important to demonstrate that regulations are effective addressing the problems created by market failures. This calls for analysis of regulatory impact to be mandated before regulations are made, and conducted periodically to measure their effectiveness. Before making a regulation, such analysis usually includes projections for several years into the future. This can help focus regulatoy resources on significant problems that are already there or are likely to arise.

3) Jurisdiction:

Jurisdiction issues could be territorial, sectoral or based on organisation-type or size.

Territorial jurisdiction issues:

The online world is truly global. Most of the applications that Indians use are hosted abroad, and offered by organisations with limited or no physical presence in India. For instance, Facebook does not have a data centre in India, and most of its software development is also done abroad. This poses difficulties for monitoring and enforcement by the proposed DPA. Establishing jurisdiction for the purposes of regulation and supervision requires having an identifier for the organisation (eg. registration), a line of communication with the organisation, being able to inspect the databases and softwares, and having an entity on whom penalties and other enforcement orders can be served. While this is relatively easy to achieve for organisations that are based in India (i.e. registered in India), it is difficult and expensive to establish jurisdiction over foreign organisations. Also, imposing costs on India-based organisations may drive these businesses out of India. The costs of establishing jurisdiction may vary depending on the type of entity. The larger question is: why would anyone agree to be regulated by a DPA in India? Whether a foreign organisation providing an online service will submit to regulations in India will depend on the disincentive of not doing so.

In finance also, for instance, there is a jurisdiction problem. It is potentially easy to get a financial service from a service provider abroad. It has been considered important to establish jurisdiction over any firm offering financial services for consumers in India. So, across sectors, there are prohibitions on offering financial services without authorisation from a regulator in India. In 2013, when recommending wide-ranging financial sector reforms, the Financial Sector Legislative Reforms Commission had also recommended that no person should be allowed to offer financial services in India without authorisation by a regulator.

China seems to have taken a similar approach for internet, and ended up creating a parallel internet for themselves, wherein a large number of websites and applications are banned simply because they do not play by the rules made by the country. One could argue that this is reasonable, as each country has the right to define what kind of internet access its citizens should have. While this right is reasonable, the costs of exercising this right are considerable, as this may lead to a large number of bans, and cut India off from larger parts of global flow of online services. So, if we want to establish jurisdiction over foreign firms collecting data from Indians, it would require creating a strong disincentive, such as a ban, for the controller/processor that does not give jurisdiction to the DPA. Even if we limit this to, say, “important” or “sensitive” personal data, it can create problems. For example, many patients from India send their medical information for second opinions from medical establishments abroad. This is usually done through some hospital in India. If the DPA insists that each such foreign establishment must register with it or such data cannot be shared, this would deny an important service to the patients.

In my view, it would be better to begin with regulating entities that are already registered in India, and have offices here. This itself will need considerable discretion to be exercised, as has been seen in controversies around “permanent establishment” in tax cases. On the margins, there will be differences of opinion about when an entity can be said to be based in India. However, giving a regulator powers to take draconian measures to establish jurisdiction over entities based overseas may lead to excessive bans, especially when the regulator has low capacity, because capacity is required to determine suitable regulatory strategies for establishing jurisdictions by other means.

Sectoral jurisdiction:

Another jurisdiction issue is sectoral. As the data protection authority will pursue its objectives across all sectors, this can raise conflicts between regulators. For example, in banking, securities markets, payments, etc, the data security issues are regulated by the respective regulators, because this is essential to these services. These services are largely operated through online systems, and a large part of prudential regulation is about ensuring security of these systems. If a payment system is breached, it would have direct financial consequence. The personal data in this case is mainly the financial data. Similar arguments can be made for other sectors as well. Another issue in this context is that there is already existing regulatory capacity in many sectors, but perhaps the present data protections in those sectors are not adequate. Perhaps, a solution that would also help reduce the capacity required in the DPA is to require the DPA to make regulations/standards in consultations with respective regulators, and once the regulations/standards have been specified, the sectoral regulators could supervise and enforce the law and the regulations. The respective regulators could do so in the course of their routine supervision of their sectors. I think this could be done for: financial firms, telecom service providers, internet service providers, etc. This may not appear to be a “clean” solution, but such aesthetic concerns should be weighed against the benefit of freeing up capacity at the DPA to focus on other sectors, and avoiding unnecessary conflicts. Also, since these regulators are in any case supervising their sectors, the additional capacity required to monitor and enforce data protection standards would probably be less than building the capacity for these sectors in the DPA.

Jurisdiction over small organisations:

I would strongly recommend exempting small organisations. Given the scale of our country, it would be impractical to seek implementation of this in every retail store and small firm. This is not to say that there are no data protection risks arising from small enterprises. But to begin with, the system should focus on achieving good outcomes without imposing costs on small organisations. Further, for the purposes of redress, only individuals and small organisations should be able to seek redress.

4) On the rights-based approach to data protection

Following the example of other countries, the Committee seems to have used the rights-baed language for most of the protections it seeks to recommend in the law. I request the Committee to think about this issue more carefully, because this has consequences for the way the regulatory system will evolve.

One way to think about this is to *distinguish between protections that are required for the market processes to function well, and the protections that are outcomes of the market process*. Informed consent is a pre-condition for the market to produce good outcomes, because such consent is necessary as an *input* to the market processes to see what the consumers want. Informed consent signals what the consumers see as useful trade-off between protecting their privacy and using their data. On the other hand, the extent to which a person is subject to a decision solely based on automated processing, and other such phenomena are outcomes of the market processes, and may only need some specific interventions by the regulator to ensure good outcomes. In my view, only the former should be given in a rights-based framwork, and other protections, if they are considered at all, may be given as objectives of the regulator to be achieved in the aggregate, rather than as rights for individual consumers.

The word "right" gives a sense that each individual can invoke the State's support to claim what is being called a right, without regard to the costs. In data protection, the right to control one's personal data is perhaps the only such right, and it can be said to include a few rights, such as informed consent, confirmation, access, and rectification, which are required to give effect to a proper right to informed consent. This "right to have control over one's personal data" should be a foundational feature of a data protection regime. The remaining protections, if any, may be given to the regulator as objectives to be achieved at aggregate level, but not given as rights to individual users. The difference this would make is that the focus of the regulator would be on achieving good outcomes in the aggregate. Individual rights-based approach should only be used for the basic rights required to give each user a reasonable control over her personal data.

Take the example of direct marketing. Firms conduct direct marketing because it connects them to persons who become their consumers, which also means that many consumers gain from the process. So, the society on the whole is better off because of direct marketing. The problem, however, is that an externality is being imposed on those who receive calls they are not interested in. Since many consumers value being let alone sometimes, there are market-based solutions to this problem. There are call filters (eg. Trucaller), email filters, etc., which are available for such consumers. Consumers can block such calls and discontinue emails and messages from particular sources. Framing this issue as an "absolute individual right", and bringing in the State's "monopoly of coercion" into this situation may be excessive, and would discourage user to solve this problem by market-based solutions. Users should put in effort to solve these problems, and they may not do that if the regulator brings coercion into the situation. However, regulator may be given an objective to improve the system of processing for direct marketing, without creating an individual right.

5) Need to distinguish between data protection and broader privacy concerns:

The Committee is mandated to "study various issues relating to data protection in India". In my view, issues such as data portability, protection against being subject to a decision based solely on automated processing, and the right to be forgotten are not strictly data protection issues. They are data-related issues, but they have little to do with protection of personal data.

- ***Data portability*** is not necessary for data protection, even though it may be good for the users to get data portability, so that they can shift from one controller/processor to another. This is a competition issue, as lack of portability hampers competition in a market.

- ***Being subject to a decision based solely on automated processing*** is, arguably, a problem. However, this is not related to protection of personal data. Automated processing can have benefits as well as costs. In the egregious examples cited in the White Paper, where certain individuals are paying a huge price for such processing, it may be better for such individuals to seek other avenues for relief, instead of creating a general right. The examples given in the White Paper (person wrongly identified as IRA leader; loss of jobs, car licenses or voting rights because of wrong identification) are of situations where the automated processing led to a mistake. In such situations, there is no incentive for the processor to penalise the person. Since these are mistakes, is State intervention by creating a general right really required? In any case, this has little to do with data protection, and if it is being considered, this is the kind of protection that must be subjected to a rigorous cost-benefit analysis.

- ***The right to be forgotten***: In the Puttaswamy judgment, only one opinion discussed this, and it cannot be reasonably considered to be the majority's opinion on the matter. EU has come to this big shift in the conceptualisation of the relationship between a person and society after a long process. Even in EU, the *right to be forgotten* was replaced by a more limited *right to erasure* in the version of the GDPR adopted by the European Parliament in March 2014. We in India should not rush into such formulations. A person should incur the costs of his or her mistakes. The general right to be forgotten imposes the costs of a person's past mistakes on others in the society, because the firms holding his personal data would have to incur the cost of removing that data. This is not a data protection issue.

6) Approach to data protection in government organisations:

In a way, data protection in government organisations is probably more important than in private organisations, because a lot of the personal data that government organisations was obtained under threat of coercion. However, experience from other sectors suggests that enforcement measures that are usually effective on private entities become less effective on government organisations. For instance, the penalties that are used by regulators to coerce the regulated entities to follow the laws/regulations/standards work less effectively with government organisations. Monetary penalties ultimately impose a loss on the taxpayers. Criminal cases are often difficult to initiate against civil servants, and in India, because of the way jurisprudence has developed, a larger number of persons working in government organisations are considered to be civil servants.

In principle, neutral application of law to both private and public sector is good, and this should be in the proposed data protection also. However, there is also a need to think about other ways of ensuring data protection in the context of government organisations. Once the DPA is established and builds capacity, it could become an advisor and reviewer on data protection policies in government organisations, so that is expertise is used to prevent mistakes from being made. The Committee could consider recommending that the law should contain an enabling provision to allow government to appoint the DPA to periodically review the data protection-related policies of government organisations, and have audits of their implementation conducted under DPA's supervision.

7) Regulations, Flexibility and Innovation

Regulatory systems work well when there are clear regulations that need to be followed, and employees of regulator, the regulated entities, and the consumers know that this is the case. Clarity and certainty are crucial. However, this rules-based system comes at the cost of flexibility. Once a regulator specifies a regulation, there can be little room for innovation that violates the regulation in word, even if it follows it in spirit. This is a perennial tension, but in data protection regulation, there is arguably a deeper tension.

At the heart of a data protection system is a trade-off between valuing one's privacy and valuing beneficial uses of one's personal data. Technology has multiplied the ways in which a person can use her personal data for deriving economic and social benefits. The use, of course, needs to be based on consent of the user. When a user is giving consent, she is supposedly making some calculation in her mind about how she may benefit from that consent. However, often, it is not obvious ex-ante what kinds and scale of benefits can be gained by sharing certain kind of data. The users may be able to make a better choice if they see examples and demonstrations. However, a robust data protection regime may limit possibilities of innovation without explicit consent. So, there can be a logjam – users may not give consent without seeing demonstration of benefits, and processors may not be able to innovate without access to a critical mass of data. The logjam is for a good reason – both data protection and innovation matter. This is just one example, and there can be many situations where regulation may restrict innovation that could have led to better solutions for both data protection and beneficial use. For instance, what kind of a notice and consent process will work is an issue over which innovative solutions can be found.

One way to overcome such problems is to create a space within the regulatory system to allow limited scale innovations, where some regulatory exemptions are given. This "regulatory sandbox" needs to be provided in the law itself. Typically, a regulatory sandbox involves giving the regulator the power to oversee a closely supervised cohort of innovations for which certain regulatory exemptions are given. Once their lessons are documented, they may lead to modifications in regulations to allow innovations. This is a participatory approach here regulator and private participants work closely to help innovation happen[8]. However, for this to happen, the law needs to empower the regulator to create these "safe spaces" for innovation that achieve the objective of data protection while enhancing productive uses of data.

8) Need for sound regulatory governance and due process to be required by law:

The law will give several powers to the DPA. There are three types of actions that the DPA will take: drafting of regulations/standards; executive functions of inspection, investigation, and recommending penalties or compounding violations; and the quasi-judicial function of adjudication of disputes. The law should provide checks and balances to ensure that these powers are used properly. This requires two types of provisions: around regulatory governance of DPA, and due process to be followed by DPA. The law should provide for a good design of the Board of the DPA.

[8] See, for instance, the regulatory sandbox overseen by the Financial Conduct Authority in the UK; https://www.fca.org.uk/firms/regulatory-sandbox

The law should give the processes and rationale for appointing or removing board members. This is important to maintain independence of the DPA. For its independence, it is important that the funding process for the DPA is given in the law. Further, for accountability, it is important that the DPA be mandated to make annual plans, and publish annual reports that include performs on the previous years' plan. Each type of regulatory action should be taken only after following due process, which should be laid down in the law. Independent authorities, such as the proposed DPA, have the power to be a judge in their own cases, i.e. they have their own officers adjudicating violations which have been investigated by the officers of the same authority. This conflict needs to be managed through checks built in the law itself.

Conclusion: Proposed formulation for the data protection law

Based on the analysis present in this note, I would like to make the following suggestions on the proposed data protection law:

1) **Protections:** Achieving informed consent should be the main focus on the law. To this end, the rights discussed under "Individual Participation Rights-I" should be included as individual rights. The DPA would then focus on building systems of regulation that ensure that the foundational requirement of informed consent is met in a variety of circumstances. This in itself is a difficult challenge in India's context, as it would require interventions in a number of sectors across the country. It would be great if the DPA is able to build capacity around solving this problem. The rights discussed under "Individual Participation Rights-II" and the "Right to be Forgotten" should not be included in this law, and may be considered to be included through amendments later. Similarly, "data minimisation" should not be included as a preventive measure.

We should first get the basics right. This means that data minimisation, data portability, right to be forgotten, right to object to processing for direct marketing, and any discrimination-related protections should not be given in the first law on this subject. Such protections require high level of sophisticated state capacity, and powers that can be easily abused or inefficiently used. They are also likely to impose high costs on the economy. Setting aside the debates about whether these protections should *ever* be included in a data protecting law, I am only suggesting not including them in the law in the first instance. In a few years, when the DPA builds capacity, and is able to deliver on the protections promised, additional protections may be debated, and introduced. Entrusting a new regulator with such an expansive mandate on day one could be a recipe for failure.

2) **Jurisdiction:** The jurisdiction should be limited to those entities that are located in India. The DPA should not be given powers to "pursue" entities to establish its jurisdiction over them. Further, in sectors where regulators conducting regular supervision are already there, the responsibility for monitoring compliance and taking enforcement actions may be given to the respective regulators. Small organisations should be exempt from the law. Further, for the purposes of redress, only individuals and small organisations should be able to seek redress.

3) Tiered system: The law should create a three categories of "services and applications" based on their importance for an average person - basic, intermediate, and optional. The law should mandate the DPA to put more resources into ensuring data protection for personal data shared for "basic services and applications”. Also, in the redress system, while considering compensations, it should be considered whether the service was basic or not.

4) Enable DPA to be the advisor/reviewer/auditor for data protection in government organisations: The law should include an enabling provision for the government to appoint the DPA for advising governement organisations on data protection policies and practices, reviewing their data protection policies and practices, and auditing implementation.

5) Allow space for innovation, without compromising on the objective of the law: The law should empower the DPA should begin and oversee a regulatory sandbox to allow limited period trials of innovations that can be exempt from certain regulations.

6) Board Composition: The DPA Board should have a majority of independent members, who may be experts, retired civil servants, consumer advocates, and others. The process of appointment as well as the grounds and process for removal of members should be laid down in the law. The Board should be required to make annual plans, and publish performance reports with annual reports every year.

7) Due process requirements in the law: While making regulations, the DPA must publish draft regulations along with a statement on the legal authority to make the regulations, a statement of the problems to be solved, and an analysis of expected impact of the proposed regulation. After comments have been received, the DPA must be required to publish all the comments received, provide a reasoned response to the comments received, get the draft regulations formally approved by the board, and then publish the regulations. In case of emergency regulation-making, the requirements of consultation and analysis of regulatory impact may be relaxed, but such regulation should lapse after six months. The DPA will perform a variety of executive functions under this law. These include: inspections, investigation, and recommending penalites or compounding violations. When investigations are envisaged they should be carried out according to written terms of investigation; carried out by an appointed investigator; finished within a pre-determined period, which may be extended by a quasi-judicial officer on a reasoned order; and carried out with least disruption to a business. Similarly for recommending penalties or compounding violations, the DPA should be guided by detailed regulations requiring the authority to show proportionality, and fairness. There must be a separate wing within DPA, which adjudicates violations. Members of such wing should not interact or report to persons carrying out or overseeing the investigation functions.